Date de réception : 23/01/2015

TO THE PRESIDENT AND MEMBERS
OF THE COURT OF JUSTICE
OF THE EUROPEAN UNION

IN CASE C-362/14

MAXIMILLIAN SCHREMS

Applicant

V.

DATA PROTECTION COMMISSIONER

Respondent

AND

DIGITAL RIGHTS IRELAND LIMITED

Amicus curiae

WRITTEN OBSERVATIONS OF APPLICANT

Maximillian Schrems, pursuant to the second paragraph of Article 23 of the Protocol on the Statute of the Court of Justice, represented by Mr. Noel J. Travers, Senior Counsel, and Mr. Paul O'Shea, Barrister, both of the Bar of Ireland, as well as by Professor Herwig Hofmann, Rechtsanwalt, of the Cologne Bar, Germany, all instructed by Mr. Gerard Rudden, Solicitor, of Ahern Rudden Solicitors, 5 Clare Street, Dublin 2, Ireland, has the honour of submitting the following written observations to the Court of Justice of the European Union on the questions referred for preliminary ruling pursuant to Article 267 TFEU by the High Court of Ireland, by orders of that Honourable Court of 16th and 25th July 2014, received at the Registry of the Court of Justice of the European Union on 26th August 2014.

TABLE OF CONTENTS[1]

I. INTRODUCTION AND OVERVIEW

1. This preliminary reference has arisen from judicial review proceedings before the High Court of Ireland, wherein Maximillian Schrems, the applicant, challenges the legality of a decision by the Irish Data Protection Commissioner ("DPC"), the respondent, not to investigate a complaint lodged on 25th June 2013. Subsequent to letters dated 25th and 26th July 2013, the DPC invoked powers under the Irish Data Protection Act 1988 ("the 1998 Act") not to investigate Mr. Schrems' complaint on the ground that it was legally unsustainable.[2] This conclusion was based the DPC's

[1] The following abbreviations will, in the interest of brevity, be used in these written observations (amongst others that are defined in the text):
CFR = Charter of Fundamental Rights of the European Union;
ECHR = European Convention on Human Rights;
ECtHR = European Court of Human Rights;
US/USA = United States/ United States of America.

[2] Formally, the DPC found that the complaint was "*frivolous and vexatious*", but, as a matter of Irish data protection law, as confirmed by the referring court, this simply has the technical meaning that the complaint could not succeed. The *bona fides* of the applicant and the genuineness of his complaint was not disputed by the DPC and, moreover, has been fully upheld by the High Court in its judgment of 18th June 2014 ("the judgment of 18 June 2014"), at para. 16, which judgment underlies the order for reference and is at Appendix 2 thereto.

view that he was 'bound' by Commission Decision 2000/520/EC of 26 July 2000 ("SHD").[3] The correctness of this view, as a matter of EU law, is central to this preliminary reference. In the SHD the Commission concluded over 14 years ago that, what are set out in Annex I thereto and described therein as the 'Safe Harbor Privacy Principles' ("SHPs"), provide adequate protection, with regard to the personal data transferred from the EU/EEA to the United States. The personal data of the applicant are transferred to the USA by Facebook Ireland Ltd ("Facebook Ireland").[4]

2. If the Commission's July 2000 conclusion in the SHD as to the adequacy of protection of personal data transferred to the USA is no longer binding on national data protection authorities ("DPAs"), like the DPC in the main proceedings, the High Court has expressed the firm view that the applicant would be entitled, under the fundamental right to privacy protected under Irish constitutional law, to succeed in his judicial review application. Thus, central to this case is whether, as a matter of EU law, the Commission's adequacy assessment in the SHD binds DPAs, notwithstanding the dramatically changed factual circumstances that have been found to exist by the High Court; *i.e.*, the "*mass and undifferentiated*" access that is available to the US National Security Authority ("NSA") and other US security agencies to the personal data that have been, and that continue to be, transferred by Facebook Ireland (among others) to the USA. The core issue raised by High Court's questions is whether, notwithstanding such generalised access to the transferred data, a DPA is obliged, as a matter of EU law, to accept that the level of protection for the privacy of such personal data remains adequate, in circumstances where the data is being transferred by data controllers that it supervises within the EU (*i.e.* Facebook Ireland in the case of the DPC in the main proceedings). The applicant submits that such possibility of 'mass and undifferentiated' access results in wholly inadequate protection of sensitive, personal data in view of the criteria established in Article 25(2) and (6) of Directive 95/46/EC due to the possibility of serious violations of his rights under Articles 7 and 8 of the CFR and Article 8 of the ECHR against which there is no adequate remedy, since *de jure* and *de facto* the SHD's provisions amount to depriving him of his right to an effective remedy protected as general principles of EU law and in Article 47 CFR.

II. LEGAL AND FACTUAL BACKGROUND

A. Factual context and order of reference of High Court

3. The applicant is an Austrian national resident in Vienna. Since 2008, he has been a user of the social media service 'Facebook', and, when establishing his Facebook

[3] Commission Decision of 26 July 2000 pursuant to Directive 95/46/EC of the European Parliament and of the Council on the adequacy of the protection provided by the safe harbour privacy principles and related frequently asked questions issued by the US Department of Commerce; OJ (2000) L 215, p 7.

[4] The data that have already been transferred include highly personal and sensitive data including regarding the applicant's sexual orientation and voting intentions.

'account', he, like other Facebook users in Europe, was "*required to enter into an agreement with Facebook Ireland Ltd.*", which, as the High Court has found, means that Facebook Ireland falls "*to be regulated by the [DPC] under the terms of the [Irish] Data Protection Acts 1988-2003*".[5] The High Court has further critically found that "*some or all data relating to Facebook subscribers resident within the EU/EEA is in fact transferred to and held on servers which are physically located in the United States*".[6]

4. Thus, the respondent DPC in the main proceedings is responsible for supervising Facebook Ireland, which controls (Article 2(d) of Directive 95/46) the data of its users. Facebook Ireland processes this data by transferring some or all of the data to servers situated at data centres that are physically located in the USA, where the data is processed by Facebook Inc. ("Facebook USA", the 'processor' under Article 2(e) of Directive 95/46). Accordingly, the impugned decision of the DPC has implications for the millions of 'Facebook' users, who, like the applicant, may be concerned by the possibility of accessing of their personal data by US security agencies under programmes and legislation such as the 'PRISM' programme and the 'FISA'.[7]

5. On learning of the revelations on the activities of the NSA, the applicant lodged a written complaint on 25th June 2013 with the DPC requesting termination of data transfers by Facebook Ireland to the US. This complaint was based, among other claims, on the rules governing data transfers to the USA under the SHD and the underlying Article 25 of Directive 95/46/EC,[8] as well as on his fundamental rights under Articles 7 and 8 CFR and Article 8 ECHR. Mr. Schrems submitted that there was a high likeliness that US authorities had used their powers under various US laws, including the FISA to gain access to data held on servers of Facebook USA (amongst other companies). The Applicant contended that it was apparent from the FISA that processors, such as Facebook USA, must make all personal data available in bulk once they receive a non-specific 'directive' to cooperate with relevant US security authorities. The applicant submitted that Facebook Ireland[9] had breached its obligations under Directive 95/46, as well as under the Irish Data Protection Acts 1988-2003 (which, *inter alia*, transpose that Directive into Irish law), by proceeding to transfer, and continue to transfer, his personal data to a country that does not provide an adequate protection. As the High Court has found, such transfers "*facilitate[e] the processing of such data by Facebook itself*".[10] Although constitutional protection of the right to privacy in the United States 'Bill of Rights'

---

[5] *Ibid.*
[6] Para. 2 of the order for reference and para. 17 of the judgment of 18 June 2014.
[7] Paras. 10 to 12 of the judgment of 18 June 2014. The FISA is the Foreign Intelligence Surveillance Act of 1978 (50 U.S.C., Ch. 36).
[8] Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data; OJ (1995) L 281, p 31.
[9] Para. 29 of the judgment of 18 June 2014.
[10] Para. 29 of the judgment of 18 June 2014.

only applies to citizens and permanent residents of the United States (or to non-residents, such as previous residents, who maintain a substantial connection with the US) ("US persons"), the applicant, who is not such a person, contended that, in any event, even US persons have no right to address the relevant 'FISA court', which operates on an *ex parte* and secret basis.[11] Thus, there is no protection of his personal data and no factual or theoretical form of judicial redress against mass generalised surveillance in the US. The referring court considered such generalised access as demonstrating: *"almost beyond peradventure – that the US security services can routinely access the personal data of European citizens which has been so transferred to the United States and, in these circumstances, one may fairly question whether US law and practice in relation to data protection and State security provides for meaningful or effective judicial or legal control".*[12]

6. Instead of investigating the applicant's complaint, the respondent DPC first argued that he had no duty to investigate complaint. Later in the proceedings he invoked s. 10(1)(a) of the 1988 Act to find that the complaint cannot succeed on legal grounds ("frivolous and vexatious" in the technical sense of that provision), which allowed him to reject it without investigation. As interpreted by the High Court, this provision effectively connects the fact that a complaint 'cannot succeed' on legal grounds, with the option for an *in limine* rejection of it and the end of any investigation by the DPC. According to the DPC, s. 11(2)(b) of the 1988 Act, as amended, requires that the question of the adequacy of the level of data protection in a third country be determined in accordance with the findings of the Commission under Article 25(6) of Directive 95/46. The DPC considered that the Commission had thereunder adopted a favourable decision with regard to the USA, to the effect that US companies that participate voluntarily in the so-called 'Safe Harbor' programme ensure an 'adequate level' of data protection regarding the data in their possession, and that this included undertakings such as Facebook USA. Thus, the DPC regarded himself as being obliged (under s. 11(2)(a) of the 1988 Act, as amended) to accept the adequacy of data protection under the 'safe harbor' system and summarily dispose of the applicant's complaint, on the basis that the complaint, if investigated, could not succeed. The DPC, furthermore, considered that the applicant lacked *locus standing* to bring the compliant, because there was no evidence that his personal data had actually been accessed by the NSA or other US security agencies.

7. The applicant challenged the aforesaid DPC decision by way of the within judicial review proceedings initiated in October 2013. The relief he seeks therein from the High Court of Ireland is a declaration that the DPC's refusal to investigate his complaint is unlawful, as well as orders compelling the DPC to investigate the complaint and quashing the decision refusing to do so. Following the initiation of his judicial review application, the applicant lodged online complaints before the US

[11] This contention has been upheld by the High Court; see para. 7(b) of the order for reference.
[12] Para. 42 of the judgment of 18 June 2014: see also para. 7(b) of the order for reference.

Federal Trade Commission ("FTC") and TRUSTe Inc. ("TRUSTe", the dispute resolution body chosen by Facebook USA under the SHPs), concerning the available access by US authorities to data held with regard to him by Facebook USA.[13] Unsurprisingly, since for the reasons developed further below both bodies lack jurisdiction to deal with such complaints, TRUSTe responded by stating that it does not have any jurisdiction in this case, while the FTC has not responded.[14]

8. In its judgment of 18 June 2014, which underlies its order for reference, the High Court first rejected (paragraphs 41-45) the DPC's *locus standi* objection. It held that, even if the applicant cannot prove that his personal data has actually been accessed in the United States, he is "*entitled to object to a state of affairs where his data are transferred to a jurisdiction which, to all intents and purposes, appears to provide only limited protection against any interference with that private data by the US authorities*". The issue of standing to complain regarding the access available by US security agencies to his personal data has, therefore, been conclusively determined, for the purpose of this reference, in favour of the applicant by the High Court.

9. The High Court then considered the applicant's position under national law with regard to the protection of the applicant's right to privacy.[15] It held that, under Irish constitutional law, for an interference with the right to privacy and, in particular, with the inviolability of the dwelling (which is engaged because, as found by the High Court, much of the private data at issue is generated within the home), it must be proportionate. However, the "*mass and undifferentiated*" accessing of personal data, such as that issue in the main proceedings, "*would not pass any proportionality test or could survive constitutional scrutiny on this ground alone*".[16] Accordingly, the referring court held that, "*if this matter were governed by Irish law, then measured by these particular constitutional standards, a significant issue would arise as to whether the United States ensures an adequate level of protection for the privacy and fundamental rights and freedoms, within the meaning of s. 11(1)(a) of the 1988 Act, such as would permit data transfers to that country*".[17] Thus, if Irish law alone were applicable, the High Court has held that the applicant's judicial review application would succeed, since "*the [DPC] could not properly have exercised his s. 10(1)(a) powers to conclude in a summary fashion that there was nothing further to investigate*".[18]

10. However, the referring court considered that the dispute in the main proceedings is only partially governed by Irish law, and that one "*must therefore turn to a consideration of the position at EU law*".[19] This was because s. 11(2)(a) of the 1998

[13] See Annexes A.2 and A.3 to these observations.
[14] *Ibid.*, at Annex A.2.
[15] Paras. 47 to 57 in particular of the judgment of 18 June 2014.
[16] Para. 12 of the order for reference.
[17] Para 14 of the order for reference, and para. 56 of the judgment of 18 June 2014.
[18] *Ibid.*, para. 12 of the order for reference.
[19] Para. 57 of the judgment of 18 June 2014.

Irish Act effects "*a renvoi*" of the wider question of the adequacy of protection for the privacy of personal data in favour of EU law, while s. 11(2)(b) thereof obliges the DPC to determine the question of that adequacy in a third country, like the USA, "*in accordance with a Community finding made by the European Commission pursuant to Article 25(6) of [Directive 95/46]*"[20]. The High Court further held that Article 3(1)(b) of the SHD does not apply in this case, because: "*While Article 3(b) of the Safe Harbour Decision allows the national authorities to direct an entity to suspend data flows to that third country, this is in circumstances where - unlike the present case - the complaint is directed to the conduct of that entity*".[21]

11. With regard to EU law, the High Court therefore considered the nub of the issue to be whether the DPC is bound, by the finding contained in the SHD concerning the adequacy of protection provided for data subjects like the applicant that is available in the USA. The High Court held that, "*the essential question which arises for determination is whether, **as a matter of European Union law**, the [DPC] is nonetheless absolutely bound by the finding of the European Commission as manifested in the [SHD] in relation to the adequacy of data protection in the law and practice of the United States having regard in particular **to the subsequent entry into force of Article 8 of the Charter**, the provisions of Article 25(6) of the 1995 Directive notwithstanding*".[22] In this respect, the High Court considers that the applicant's real objection concerns not the conduct of Facebook Ireland, as such, but "*the fact that the Commission has already determined that US law and practice provided adequate data protection in circumstances where it is clear from the Snowden disclosures that personal data of EU citizens so transferred to the US can be accessed by the US authorities on a mass and undifferentiated basis.*"[23]

B. Core applicable EU law provisions

(i) Right to privacy, data protection, an effective remedy and to a fair trial

12. The right to privacy and data protection is protected under Articles 7 and 8 of the CFR. In cases arising prior to the entry into force of the CFR, from the general principles of Union law (Article 6(3) TEU). Article 6(3) TEU further provides that the "*constitutional traditions common to the Member States*" and the fundamental rights guaranteed by the ECHR "*constitute general principles*" of EU law. Specifically, with regard to the protection of personal data, Article 16(1) TFEU explicitly and unequivocally provides that: "*Everyone has the right to the protection of personal data concerning them.*" Protection is offered against public and private infringements.

---

[20] Para. 16 of the order for reference.
[21] Para. 19 of the order for reference.
[22] *Ibid.*, in the quotes from paras. 69-70 of the judgment of 18 June 2014 (emphasis in original).
[23] Para. 19 of the order for reference.

13. It is firmly established, that these fundamental rights place a duty on Member States and the Union reasonably to protect data subjects against violations by third parties. In addition to the substantive right to protection, Article 8(3) CFR also guarantees the procedural right to the supervision by an independent authority. The Court has held, in this regard, that: "*It was established not to grant a special status to those authorities themselves as well as their agents, but in order to strengthen the protection of individuals and bodies affected by their decisions*".[24]

14. The right to an effective remedy is protected under Article 47 CFR, and by Article 6(3) TEU in combination with Article 6 ECHR.[25] It is a general principle of EU law which comprises an essential component of ensuring respect for the rule of law (Article 2 TEU).[26] It is explicitly recognised and has been restated as the right to an 'effective remedy before a tribunal' in Article 47 CFR.

(ii) Directive 95/46

15. Under Article 1(1) of Directive 95/46, the objective of the Directive is stated to be the protection of "*the fundamental rights and freedoms of natural persons, and in particular their right to privacy with respect to the processing of personal data*".

16. Chapter IV, comprising Articles 25-26, of Directive 95/46 is concerned with the 'Transfer of Personal Data to Third Countries'. The principles governing such transfers are set out in Article 25. Article 26 of Directive 95/46 requires that "*Member States shall provide that a transfer or a set of transfers of personal data to a third country which does not ensure an adequate level of protection within the meaning of Article 25 (2) may take place*", once certain conditions are met amongst which, at indent (d), is the condition that "*the transfer is necessary or legally required on important public interest grounds*".

17. Member States are required, under Article 25(1), to ensure in respect of transfers of personal data "*which are undergoing processing or are intended for processing after transfer*" is that "*the third country in question ensures an adequate level of*

---

[24] Case C-518/07 *Commission v Germany* [2010] ECR I-1885, para. 25.

[25] The Court has repeatedly found this right to be a fundamental right of individuals resulting from the common constitutional traditions of the Member States and recognised in Articles 6 and 13 ECHR. The fundamental rights arising from this are, thus, also protected as general principles of EU law under Article 6(3) TEU: see e.g.: Case 222/84 *Johnston* [1986] ECR 1651, paras 18 and 19; Case 222/86 *Heylens and Others* [1987] ECR 4097, para 14; Case C-424/99 *Commission v Austria* [2001] ECR I-9285, para 45; Case C-50/00 P *Unión de Pequeños Agricultores v Council* [2002] ECR I-6677, para 39; Case C-467/01 *Eribrand* [2003] ECR I-6471, para 61; Case C-432/05 *Unibet* [2007] ECR I-2271, para 37; Joined Cases C-402/05 P and C-415/05 P *Kadi and Al Barakaat* [2008] ECR I-6351, para 335; Case 12/08 *Mono Car Styling* [2009] ECR I-6653, para 47; Joined Cases C-317/08 to C-320/08 *Alassini* [2010] ECR I-2213, para 61.

[26] The recognition of which in the Union legal order dates back to Case 294/84 *Les Verts* [1986] ECR 1339, paras 23, 24. The relation between the right to an effective judicial remedy and the rule of law is outlined in Case C-50/00 P *Unión de Pequeños Agricultores v Council* [2002] ECR I-6677, paras 38-39.

protection". With regard to the required adequacy, Article 25(2) provides that:

> *"The adequacy of the level of protection afforded by a third country shall be assessed in the light of all the circumstances surrounding a data transfer operation or set of data transfer operations; particular consideration shall be given to the nature of the data, the purpose and duration of the proposed processing operation or operations, the country of origin and country of final destination, the rules of law, both general and sectoral, in force in the third country in question and the professional rules and security measures which are complied with in that country."*

18. The Commission is given a specific role under Article 25(4) and (5), where it "*finds*" that "*a third country does not ensure an adequate level of protection within the meaning of [Article 25(2)]*" of entering into negotiations "*with a view to remedying the situation*". Article 25(6) then provides:

> *"The Commission may find, in accordance with the procedure referred to in Article 31(2), that a third country ensures an adequate level of protection within the meaning of paragraph 2 of this Article, by reason of its domestic law or of the international commitments it has entered into, particularly upon conclusion of the negotiations referred to in paragraph 5, for the protection of the private lives and basic freedoms and rights of individuals.*
>
> *Member States shall take the measures necessary to comply with the Commission's decision."*

(iii) Commission Decision 2000/520/EC of 26 July 2000 ("the SHD")

19. Under Article 1(1) of the SHD:

> *"For the purposes of Article 25(2) of Directive 95/46/EC, for all the activities falling within the scope of that Directive, the 'Safe Harbor Privacy Principles' (hereinafter 'the Principles), as set out in Annex I to this Decision, implemented in accordance with the guidance provided by the frequently asked questions (hereinafter 'the FAQs') issued by the US Department of Commerce on 21 July 2000 as set out in Annex II to this Decision are considered to ensure an adequate level of protection for personal data transferred from the Community to organisations established in the United States, having regard to the following documents issued by the US Department of Commerce".*

The list of documents refers to four documents contained in Annexes III to VI of the SHD.

20. Under Article 3(1) of the SHD, the competent DPAs:

> *"may exercise their existing powers to suspend data flows to an organisation that has self-certified its adherence to the Principles implemented in accordance with the*

FAQs in order to protect individuals with regard to the processing of their personal data in cases where:

...

(b) there is a substantial likelihood that the Principles are being violated; there is a reasonable basis for believing that the enforcement mechanism concerned is not taking or will not take adequate and timely steps to settle the case at issue; the continuing transfer would create an imminent risk of grave harm to data subjects; and the competent authorities in the Member State have made reasonable efforts under the circumstances to provide the organisation with notice and an opportunity to respond."

C. Questions referred & provisional view of High Court

21. In its judgment of 18 June 2014, the High Court decided to adjourn the proceedings before it and refer two questions pursuant to Article 267 TFEU, which it subsequently formulated in the order for reference. In doing so, it has defined the core issue of Union law underlying the reference as being whether, having regard to its "*findings of fact regarding the Snowden disclosures and the subsequent entry into force of Article 7 and Article 8 of the Charter*", as well as this Court's recent judgment in ***Digital Rights Ireland***,[27] the DPC was bound by the determination made by the Commission in the SHD "*as to the adequacy of the data protection offered by US law and practice*", or may it, particularly in the light of the subsequent entry into force of the CFR, look "*behind that Community finding*" or even "*disregard*" it.[28]

22. Prior to making the reference, the High Court heard an application, on 2nd July 2014, from Digital Rights Ireland to intervene in this case as an *amicus curia*, to which application it acceded on 16th July 2014.[29] By order of the same date, the High Court ordered that the two questions set out immediately below be referred to this Court.

> *"Whether in the course of determining a complaint which has been made to an independent office holder who has been vested by statute with the functions of administering and enforcing data protection legislation that personal data is being transferred to another third country (in this case, the United States of America) the laws and practices of which, it is claimed, do not contain adequate protections for the data subject, that office holder is absolutely bound by the Community finding to the contrary contained in Commission*

---

[27] Joined Cases C-293/12 and C-594/12 *Digital Rights Ireland v. Minister for Communication Marine and Natural resources & Others and Kärntner Landesregierung and Others* (Grand Chamber) ECLI:EU:C:2014:238 of 8 April 2014.

[28] Para. 21 of the order for reference, and paras. 70 and 84 of the judgment of 18 June 2014.

[29] It also acceded, on 16 July 2014, to an application made by Mr. Schrems, on 4 July 2014, for a 'protective costs order'. Thus, the High Court has ordered, for the applicant's benefit, that he be limited to a maximum of €10,000 costs in the proceedings should be ultimately not succeed and costs be awarded against him, although the High Court indicated that it would be unlikely that coats would be awarded again the applicant given the clear public interest of the issues raised by his judicial review application.

Decision of 26 July 2000 (2000/520/EC) having regard to Article 7, Article 8 and Article 47 of the Charter of Fundamental Rights of the European Union (2000/C364/012), the provisions of Article 25(6) of Directive 95/46/EC3 notwithstanding?

Or, alternatively, may and/or must the office holder conduct his or her own investigation of the matter in the light of factual developments in the meantime since that Commission Decision was first published?"

23. The High Court sets out its provisional views as to the possible responses this Court might give to the questions referred in the final section (paragraphs 23-27) of its order for reference. It considers it difficult to see how the SHD, at least viewed in the abstract, could satisfy the requirements of Articles 7 and 8 of the CFR, especially having regard to the principles enunciated in ***Digital Rights Ireland***,[30] given the potentially generalised access by the US authorities to personal data transferred to the USA without any oversight having been carried out within the EU prior to the transfers taking place. Furthermore, the guarantee of the inviolability of the home as a "*place of repose from the cares of the world*" would, the High Court considers, be compromised, "*if it were thought that electronic communications often emanating within the home could be accessed by State authorities ... on a casual or generalised basis without the need for objective justification based on considerations of national security or the prevention of crime specific to the individual or individuals concerned and attended by appropriate and verifiable safeguards.*"[31] Finally, the High Court observes that this Court might consider, in the light of ***Digital Rights Ireland***, whether an interpretation of Directive 95/46, and especially of Article 25(6) thereof along with the SHD, would be open, such as would effectively permit a DPA, like the DPC in this case, not to be bound by the SHD and allow it to investigate whether privacy protection in the US satisfies the requirements of Articles 7 and 8 of the CFR.

III. ANALYSIS

A. Overview

24. It is clear from the order for reference that the key question raised is whether the administrative finding made by the Commission in the SHD to the effect that self-certification under the SHPs provides adequate protection of the personal data transferred from the EU to servers situated within the jurisdictional control of the US authorities **remains valid**. This question has arisen in circumstances where it has become clear within the last 18 months that that the personal data so transferred to the US is accessible by the US authorities on a "*mass and undifferentiated*" basis without any effective legal remedy.

---

[30] Joined Cases C-293/12 and C-594/12, loc. cit., n. 27 above.
[31] Para. 24 of the order for reference.

25. The applicant submits that there can only be one answer to this core question that would vindicate his fundamental rights, *i.e.* that Union law does not preclude DPAs, like the DPC in the main proceedings, from investigating and making findings on foot of complaints that third countries to which data are transferred from the EU do not respect fundamental rights guaranteed under Union law. The applicant's case is not, however, that there can never be access to such transferred data. Instead, he submits that such access cannot, under Union law for the specific reasons developed below, be countenanced where it occurs "*on a casual or generalised basis without the need for objective justification based on considerations of national security or the prevention of crime specific to the individual or individuals concerned and attended by appropriate and verifiable safeguards*".[32]

26. In the light of the High Court's findings of fact with regard to the access by US security agencies to data transferred to the USA, the principles relating to the fundamental right to privacy and data protection that this Court so cogently confirmed in ***Digital Rights Ireland*** with regard to data retention within the Union apply even more forcefully to data transferred to third countries whose authorities are outside the control of Union law.[33] In particular, the applicant submits that this Court should confirm the fundamental nature of the right to privacy and data protection in EU law, and in particular that this right may not be derogated from by the Commission when considering the adequacy of the laws and practices of third countries with regard to protecting the privacy and protection of personal data transferred to such countries.

27. Overall, the level of protection afforded to the applicant should not be lower under Directive 95/46, as further implemented by the SHD, than is required under the CFR. Moreover, it would be a highly regressive step for European integration if the referring court were precluded from vindicating the applicant's rights to privacy and data protection under Irish constitutional law due to a dramatically lower standard of protection being applicable under EU law on foot of an administrative assessment made over 14 years ago by the Commission in the SHD as to what constitutes adequacy of protection. In this respect, the applicant observes that a similar right to privacy to that he enjoys under Irish constitutional law is recognised under Austrian constitutional law.[34]

28. By way of introduction, the applicant submits that DPAs, like the DPC, cannot, under

---

[32] This Court has confirmed in a consistent line of case-law stretching from Case 6/64 *Costa v ENEL* [1964] ECR, English special edition, p. 585, the division of jurisdiction between it and national courts in the preliminary reference procedure between. As it held more recently, for instance, in Case C-140/09 *Traghetti del Mediterraneo* [2010] ECR I-5243,: "*[it] has no jurisdiction to give a ruling on the facts in an individual case or to apply the European Union law rules which it has interpreted to national measures or situations, since those questions are matters for the exclusive jurisdiction of the national court*" (at para. 22, emphasis added). Thus, in the context of this preliminary reference procedure, the facts are exclusively for the national court to determine.

[33] Joined Cases C-293/12 and C-594/12, loc. cit., n. 27 above.

[34] See, in particular, the judgment of the Austrian Constitutional Court on 'Data Retention', G 47/2012-49, G 59/2012-38, G 62/2012-46, G 70/2012-40, G 71/2012-36 of 27 June 2014.

Article 3(1)(b) SHD, protect his rights and those of other Facebook users by suspending the data flows from Facebook Ireland to Facebook USA. Article 3(1)(b) requires four cumulative conditions to be fulfilled before a data flow suspension may be directed by a DPA,[35] of which the applicant considers the first cannot be fulfilled. That first condition of Article 3(1)(b), like the 'chapeau' of Article 3(1) SHD, refers to a violation of "the Principles" (in capital letters). The principles are defined in Article 1(1) of the SHD as the SHPs "*set out in Annex 1 to this Decision*". This means that Article 3(1)(b) expressly refers to the SHPs in the annexed text, rather than any other (general) legal principles of EU law. Facebook USA, as a self-certifying body to which data are transferred has not itself violated the SHPs as a result of the 'mass and undifferentiated' access to the data it holds by US authorities, as the SHPs are expressly limited by US law, which paragraph 4 in Annex I to the SHD defines by reference to statute, government regulation, or case law. The crucial point is that the SHPs are not themselves EU law principles, but merely an annexed foreign legal text. The SHD is best described as a mere European 'wrapper' over inherently US legal texts, namely the FAQs and letters in Annexes I to VII to the SHD. An interpretation of the annexed text in the light of EU law would be inconsistent with the legal nature of the 'Safe Harbor' system, which is simply a US self-certification programme, recognised by the Commission. Interpreting this US system under EU law, would be like reinterpreting the law of other sovereign countries (which were found 'adequate' by the Commission) under Union law, while these countries are naturally following their own interpretation.[36]

B. Invalidation of the SHD

29. The applicant submits that the SHD should be found invalid by this Court for the following reasons:

(i) Incompatibility of the SHD with Article 25 of the Directive 95/46

30. The SHD is incompatible with Article 25(6) of Directive 95/46, its legal basis. Firstly, it does not comply with the conditions of the provision, which allow the Commission to find that a third country such as the USA "*ensures adequate protection*" by reason "*of its domestic law or of the international commitments it has entered into*". The Commission thereby has to assess the level of protection provided in a third country. It has to take into account, in particular, factors such as the legal and factual level of protection. For the reasons developed in detail by Professor Böhm

[35] That the conditions are cumulative is, the applicant submits, clear from the punctuation of the provision (the use of semi colons after each condition) and the use of "*and*" by way of introduction to the fourth condition. The cumulative nature of the conditions also emerges equally clearly from at least the French and German texts of Article 3(1)(b) SHD.

[36] The High Court has reached the same conclusion as to the non-applicability of Article 3(1)(b) of the SHD in this case, but on foot of different reasoning: see para. 10 above.

in her opinion contained in **Annex 1** to these observations, the applicant submits that the Commission could not reasonably have formed its opinion in the SHD in July 2000 to an adequate level of protection based on the SHPs in combination with existing US domestic law.[37] The differences in levels of protection provided by EU law, on one hand, and by the SHPs regime, on the other, are, the applicant submits, by reference to Professor Böhm's analysis in her opinion in Annex 1, so numerous and substantially so serious to allow rationally for a finding of adequacy. The Commission therefore committed a manifest error of assessment which would justify this Court invalidating the SHD. In support of this submission, the applicant would, in particular, refer the Court to the following reasons.

31. Firstly, the conditions of Article 25(6) Directive 95/46 were not fulfilled. In order to adopt the SHD on the basis of the SHPs, the Commission must have understood the SHPs as "*international commitments*" entered into by the US under Article 25(6) following negotiations under Article 25(5) of Directive 95/46. However, it is submitted that the 'safe harbor' regime (comprised of the SHPs and the 'Frequently Asked Questions' ("FAQs")) do not amount to an international commitment by the US Government, but merely to a publication of a US government department (the US Department of Commerce) that offers a code of behaviour allowing private parties to engage in more or less supervised commitments on their part as to the protection and security of the personal data they control under a self-certification structure that is primarily supervised by private arbitration.

32. In essence, individual private companies and organisations can voluntarily declare that they intend to comply with the code in their capacity as data controllers. This cannot constitute "*an adequate level of protection ... by reasons of [the US's] domestic law or of the international commitments it has entered into*" (emphasis added) for the purpose of Article 26(6) of Directive 95/46. Consequently, the applicant submits that the Commission erred in law in concluding that it was entitled to make a finding of adequacy in the SHD on the basis of Article 25(6). The finding of adequacy in the SHD decision is, thus, invalid and not binding on DPAs like the DPC.

33. Secondly, and more substantively, the applicant submits that the SHD and the SHPs fall short in view of regulatory content. Thus, Directive 95/46 defines in Article 2(b), as modes of processing of data: "*any set of operations, which is performed upon personal data, whether or not by automatic means, such as collection, recording, organisation, storage adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, blocking, erasure or destruction.*" The SHD limits, by stark contrast, only the transfer to a third party and the change of purpose. Any other form of

[37] An in-depth analysis of the inadequacy of the SHD by comparison to EU data protection law is set out, for the assistance of the Court, in the opinion of Prof. Dr. Franziska Böhm of the University of Münster (Germany): see Annex A.1.

processing, even of data of the most personal and thus sensitive nature, can be processed without meaningful limitations. The applicant submits that the SHD is therefore incapable of providing an adequate level of protection in the sense of Article 25(1) and (2) of Directive 95/46.

34. Consequently, the applicant submits that the Commission erred in law in concluding that it was entitled to make a finding of adequacy in the SHD on the basis of Article 25(6). The finding of adequacy in the SHD decision is thus invalid and not binding on DPAs like the DPC.

(ii) Incompatibility of the SHD with fundamental rights protection in EU law

35. It is appropriate initially to recall that the High Court has already found that the standard of protection of privacy currently available to the applicant in the context of the exiting SHD is grossly inadequate compared with the protection of the right of privacy the applicant enjoys as a fundamental right under Irish constitutional law. Furthermore, the applicant submits that, as an Austrian national and resident, he also enjoys rights under the Austrian constitutional law, which recognises and applies the standard of privacy protected under Article 8 of the ECtHR and the right to data protection in section 1 of the Austrian *Datenschutzgesetz*, as directly applicable constitutional rights.[38] These standards would not permit the generalised accessing of personal data such as that issue in the main proceedings that has been found by the referring court to occur in the USA. The high level of protection of privacy that the applicant enjoys under national law in at least Ireland and Austria (amongst, in all likelihood the applicant submits, many other Member States) is a factor that he, respectfully submits, should be borne in mind by this Court in considering the scope of the protection of the privacy of his personal data under EU law, both under the CFR and under the general principles of EU law.

a) Right to privacy under Directive 95/46

36. Any measure taken on the basis of Directive 95/46 must comply with the standards of protection established by the EU-protected fundamental rights. Such rights arise both from the CFR (Article 6(1) TEU) and, in cases arising prior to the entry into force of the CFR, from the general principles of Union law (Article 6(3) TEU). Article 6(3) TEU further provides that the fundamental rights guaranteed by the ECHR "*constitute general principles*" of EU law. Specifically, with regard to the protection of personal data, Article 16(1) TFEU explicitly and unequivocally provides that: "*Everyone has the right to the protection of personal data concerning them.*"[39]

---

[38] See the Austrian Constitutional Court's 'Data Retention; judgment of 27 June 2014, cited in n. 34 above.

[39] In *Digital Rights Ireland*, the Court confirmed the close link between the CFR and the ECHR in data protection related cases.

37. According to Article 1(1) of Directive 95/46, its objective is to protect the *"fundamental rights and freedoms of natural persons, and in particular their right to privacy with regard to the processing of personal data"*. In this respect, it should also be noted that recital 10 in the preamble thereto states that *"the principles of the protection of the rights and freedoms of individuals, notably the right to privacy, which are contained in this Directive, give substance to and amplify those contained in [Convention No. 108 of 1981]."*

38. The SHD, which is based on Article 25(6) of Directive 95/46, regulates the transfer of personal data to the USA, while the SHPs in Annex I thereto limit the subsequent use there of the data. The SHD therefore falls to be reviewed with regard to its compliance with the requirements of Articles 7 and 8 CFR, which fall to be interpreted, as this Court has held in ***Digital Rights Ireland***, in a parallel way to the requirements flowing from Article 8 ECHR.

b) Scope of right to privacy with regard to processing of personal data in EU law

39. It is clear from Articles 7 and 8 CFR that protection of personal data is offered as against both public and private infringements. This is clear from the wording of Article 8 CFR, which calls for an independent supervisory authority (Article 8(3)) to review potential infringements, and from the formulation of Article 8(2) CFR, which makes clear that both public and private infringements of the right are within the scope of protection. The applicant submits that the express right to the protection of personal data specified in Article 16(1) TFEU has the same scope.

40. According to the requirement of minimal protection in Article 52(3) CFR, the rights flowing from Articles 7 and 8 CFR fall to be construed as containing the minimum level of protection required by Article 8 ECHR, which guarantees, amongst others, the right to respect for private and family life. The rights defined in Articles 7 and 8 CFR are a restatement of the rights accepted as general principles of EU law as they were in force at the time of the adoption of Directive 95/46 and the SHD in 2000. The two sources of fundamental rights protection may therefore be treated together in the discussion of privacy and the protection of personal data.

41. It is well established that the processing of data is covered by both the right to privacy and the right to the protection of personal data under Articles 7 and 8 CFR.[40] In fact, the right to the protection of personal data has its roots in the protection of privacy. Thus, in ***Digital Rights Ireland***, the Court held that *"the protection of personal data resulting from the explicit obligation laid down in Article 8(1) of the Charter is especially important for the right to respect for private life enshrined in Article 7 of*

[40] See Cases C-92/09 and C-93/09 *Volker und Markus Schecke and Eifert* [2010] ECR I-11063, paras 47, 52; and Joined Cases C-293/12 and C-594/12 *Digital Rights Ireland*, loc. cit. n. 27 above, para 29.

the Charter".[41] The Court explained its approach as follows in the *Schwarz* case:

> *"Article 7 of the Charter states, inter alia, that everyone has the right to respect for his or her private life. Under Article 8(1) thereof, everyone has the right to the protection of personal data concerning him or her. It follows from a joint reading of those articles that, as a general rule, any processing of personal data by a third party may constitute a threat to those rights. From the outset, it should be borne in mind that the right to respect for private life with regard to the processing of personal data concerns any information relating to an identified or identifiable individual."*[42]

42. With regard to the notion of interference of these rights, the Court has held that, to establish the existence of an interference with the fundamental right to privacy under Article 7 CFR, *"it does not matter whether the information on the private lives concerned is sensitive or whether the persons concerned have been inconvenienced in any way"*: the communication of collected personal data to third parties, be they public authorities or private parties, constitutes interference with the right to privacy, *"whatever the subsequent use of the information thus communicated"*.[43] Furthermore, in ***Digital Rights Ireland***, the Court confirmed that, permitting access by competent national authorities to such data, constitutes an additional, discrete interference with that fundamental right.[44] Moreover, any form of processing of personal data is protected by Article 8 CFR and constitutes an interference with this right.[45] Given the nature of exchange between friends and family on Facebook, and that such data includes personal information, the applicant submits that the review of the Commission's assessment as to the adequacy of protection in the SHD should be carried out against the combined criteria of Articles 7 and 8 CFR.

43. Interference by processing takes place in various contexts. Facebook USA processes personal data by storing and using the data of its users for commercial purposes. The company establishes user profiles and sells some results of the analysis of profiles to clients. Furthermore, Facebook Ireland processes data by transferring the users' personal data (such as photos, mails and messages, bibliographical data and social relations, expressions of 'likes' or 'following' of sources of information) to the data centres of its parent company, Facebook USA, in the USA[46] For the purpose of the

---

[41] *Ibid.*, para 53.

[42] Case C-291/12 *Michael Schwarz v Stadt Bochum* ECLI:EU:C:2013:670 of 17 October 2013, paras. 24-26, citing Joined Cases C-92/09 and C-93/09 *Volker und Markus Schecke and Eifert*, loc. cit, n. 39, para. 52, and Joined Cases C-468/10 and C-469/10 *ASNEF and FECEMD* [2011] ECR I-12181, para. 42.

[43] Joined Cases C-465/00, C-138/01 and C-139/01 *Österreichischer Rundfunk & Others* [2003] ECR I-4989, paras. 74-75.

[44] *Digital Rights Ireland*, at para. 35. The Court referred to Article 8 of the ECHR, and the ECtHR case-law in *Leander v. Sweden*, 26 March 1987, § 48, Series A no 116; *Rotaru v. Romania* [GC], no. 28341/95, § 46, ECHR 2000-V; and *Weber and Saravia v. Germany* (dec.), no. 54934/00, § 79, ECHR 2006-XI).

[45] *Digital Rights Ireland*, at para. 36.

[46] Transfer of data constitutes processing in EU law. Thus, Article 2(b) of Directive 95/46 defines 'processing of personal data' ('processing') as: *"any operation or set of operations which is performed upon personal data, whether or not by automatic means, such as collection, recording, organization, storage, adaptation or alteration, retrieval, consultation, use, **disclosure by transmission**, dissemination or otherwise making*

complaint at issue in the main proceedings the central matter is the transfer of data from Facebook Ireland to Facebook USA, in the light of the generalised accessibility of the data stored at Facebook USA to the NSA and other US security agencies under powers they enjoy under domestic US legislation.[47]

44. The issue which arises is not dissimilar to but more serious than that considered by the Court in the ***Digital Rights Ireland*** with regard to the Data Retention Directive.[48] In that case, the Court held that the interference was a particularly serious one, because of the wide-ranging consequences and because the persons concerned were not informed of the processing, which could create "*in the minds of the persons concerned the feeling that their private lives are the subject of constant surveillance*".[49] In this case, the interference is far graver as the data at issue is being transferred beyond the protection of EU law, and:

- At least all non-US Facebook users are concerned, amongst them the applicant.[50]
- European users remain largely uninformed about the fact that their individual data, including the content of their 'private; conversations, will be generally accessible by US security agencies.
- Although such users signed the general terms and conditions with Facebook, those terms do not specify that their personal data has been or will be accessed by US security agencies in specific cases, such that European Facebook users could not expect that their posts, for instance, could be routinely accessed by the NSA in the context of mass and undifferentiated access.[51]
- The amount of the data concerned is enormous and this, combined with the secret access by the NSA and others, renders the interference extremely serious.
- The referring court has found that within the USA, for data transferred from Facebook Ireland, "*EU citizens have no effective right to be heard on the question of the interception and surveillance of their data*".[52] The relevant 'FISA court' operates "*on an ex parte and secret basis. EU citizens have no effective right to be heard on the question of the interception and surveillance of their data*".[53]

---

available, alignment or combination, blocking, erasure or destruction" (emphasis added).

[47] Most notably, under s. 215 of the Patriot Act, s. 702 of the FISA, as amended, and Presidential Executive Order 12333.

[48] Directive 2006/24/EC of the European Parliament and of the Council of 15 March 2006 on the retention of data generated or processed in connection with the provision of publicly available electronic communications services or of public communications networks and amending Directive 2002/58/EC (OJ 2006 L 105, p. 54).

[49] Para. 37.

[50] It appears from Facebook's commercial claims that 82% of its users are outside of the US and Canada. It is, therefore, likely that the personal data of all such users is managed (and thus transferred to Facebook Inc in the US) by Facebook Ireland.

[51] The relevant US law does not require probable cause or other reasons to access the information, which could potentially satisfy the requirements set out in ***Digital Rights Ireland***, at paras. 39- 40.

[52] Para. 7(b) of the order for reference.

[53] Para. 7(b) of the order for reference. By contrast, in ***Digital Rights Ireland***, this Court held (para. 62) that "*above all*" one of the failings of the Data Retention Directive was that access by the DPAs to the data retained was "*not made dependent on a prior review carried out by a court or by an independent administrative body whose decision seeks to limit access to the data and their use to what is strictly necessary*".

c) Limitation of rights guaranteed by Articles 7 and 8 CFR

45. Any limitation of the rights established by Articles 7 and 8 CFR requires justification under the criteria of Article 52(1) CFR. Accordingly, limitations must "*be provided for by law and respect the essence of those rights and freedoms.*" Furthermore, limitations have to be proportionate and may be made to rights protected under Articles 7 and 8 CFR "*only if they are necessary and genuinely meet objectives of general interest recognised by the Union or the need to protect the rights and freedoms of others*".[54] The applicant submits that the interference involved does not respect the essence of the rights at issue and is manifestly disproportionate.

46. In ***Digital Rights Ireland***, the Court clarified that **the essence** of Article 7 CFR comprises "*the acquisition of knowledge of the content of the electronic communications as such*". Accordingly, the essence of Article 8 CFR is violated when a person is stripped of any protection of personal data, especially if none of the conditions of Article 8(2) CFR, *i.e.* of purpose specification, access to collected data and rights of rectification, is fulfilled. In ***Weber and Saravia v. Germany***, the ECtHR recognised the importance of a notification in the context of surveillance measures, because it permits the individuals affected to be informed of surveillance measures and, if they wish, more effectively to challenge the legality of such measures; *i.e.*, effectively to exercise a remedy against such measures.[55] This Court has upheld in ***Digital Rights Ireland*** the importance of information as the minimum safeguard required to counter the concern of constant surveillance.[56]

47. The US Government's programmes allow, according to the findings of the High Court, full-scale access to content information, including highly personal and sensitive information. Under US law, the NSA and other US security agencies have potential access to the content of all the transferred data. This is exacerbated by the secrecy of the 'PRISM' programme, and the prohibition under US law on participating organisations from informing data subjects about the accessing of their data, as well as by the fact that no probable cause is required before the US security authorities may deliver a 'directive' to a self-certified 'safe harbor' organisation like Facebook USA requiring bulk access to the data. Worse still is the fact that the US authorities, according to the Snowden disclosures, not only have access to the data stored at Facebook USA, but also to that at a vast number of other telecom, IT or internet providers. This personal information stems not only from the applicant's use of certain services, but may also be gathered by these services themselves, or submitted by third parties (e.g. other users of such services). Thus, systems like X-Keyscore, according to the findings of the High Court, allow the US authorities to

[54] Joined Cases C-293/12 and C-594/12, ***Digital Rights Ireland***, at para. 38.
[55] No. 54934/00 of 29 June 2006.
[56] Para. 37.

access and merge this information. This results in vast amounts of personal information about most users of online services being available to the US authorities.

48. In summary, it is difficult to imagine more-clear cut and egregious violation of the essence of the rights to privacy and data protection in that neither privacy nor data protection is respected. Therefore, Article 25 of Directive 95/46 cannot be interpreted to allow the Commission to find a system which leaves the possibility of such violations of fundamental rights unsanctioned as an "*adequate level of protection*". The applicant therefore submits that the SHD is invalid on these grounds.

d) Proportionality

49. The applicant further submits that the general accessibility to the NSA and other US security agencies of the transferred data of the applicant also constitutes a manifestly disproportionate interference with his right to privacy and data protection. It is well established that, to be proportionate under Article 52(1) CFR, a restriction or limitation must be necessary "*genuinely to meet objectives of general interest recognised by the Union or the need to protect the rights and freedoms of others*".[57] The Court has summarised the relevant requirements arising from Article 52(1) CFR for assessing proportionality as being that measures adopted by Union institutions "*do not exceed the limits of what is appropriate and necessary in order to attain the objectives legitimately pursued by the legislation in question; when there is a choice between several appropriate measures recourse must be had to the least onerous, and the disadvantages caused must not be disproportionate to the aims pursued*".[58]

50. The Commission's assessment under Article 25(6) Directive 95/46 of the adequacy of protection offered by third countries with regard to the level of protection afforded by Articles 7 and 8 CFR is based on factual assessments. In exercise of its mandate under Article 25(6) Directive 95/46, the Commission acts within a set of clearly defined criteria established by the Directive. It thereby adopts an administrative decision applying legislative criteria to a given set of facts. Such decisions are subject to full review by the Court as to the proportionality of the assessment, which in the main proceedings concerns the Commission's assessment as to the adequacy of protection afforded by the US "*by reason of its domestic law or of the international commitments it has entered into*".[59] The Court therefore has full jurisdiction to review the proportionality of the Commission's assessment of the adequacy of the US legal protections. Furthermore, it is clear from ***Digital Rights Ireland*** that the protection of the fundamental right to respect for private life requires that "*derogations and*

[57] Case C-292/97 *Karlsson* [2000] ECR I-2737, para. 45.
[58] Case C-283/11 *Sky Österreich* (Grand Chamber), ECLI:EU:C:2013:28, para. 50.
[59] In addition to recognising the SHPs of the US Department of Commerce, the Commission has recognised, under Article 25(6) of Directive 95/46, Andorra, Argentina, Australia, Canada (commercial organisations), Switzerland, Faeroe Islands, Guernsey, Israel, Isle of Man, Jersey, New Zealand, Uruguay and as providing adequate protection. Data transfers to all other third countries are governed by Article 26 of the Directive.

limitations in relation to the protection of personal data must apply only in so far as is strictly necessary".[60] Moreover, the more serious the interference with the right to privacy the more reduced is the institution's discretion.[61]

51. In the main proceedings, the High Court has found the interference to be a high-end, extremely serious one involving the potential of "*mass and undifferentiated*" access by US security authorities of the personal data of Facebook users including the applicant following the transfer of their data to the USA.

Public Interest Pursued by the SHD

52. The public interest pursued by Article 25 of Directive 95/46 is to ensure such cross-border flows of personal data as "*are necessary to the expansion of international trade*", which recital 56 of Directive 95/46 states to be an objective of the Directive. The applicant submits, however, that it cannot be in the public interest pursued by Article 25 of Directive 95/46 or the SHD to allow data transfers to provide foreign intelligence information for espionage, national security or law enforcement purposes of a third country. Such data transfers are the subject of mutual assistance agreements.

53. Furthermore, it cannot be appropriate and necessary to permit extremely serious limitations of fundamental rights to ensure a marginally higher level of trade. In any case, the Commission nowhere indicated in the SHD why such limitations might be necessary and capable of fostering the trade-related objective of Directive 95/46. Instead, recital 4 of the SHD states as objective of the decision not to "*arbitrarily or unjustifiably discriminate against or between third countries where ... conditions prevail nor constitute a disguised barrier to trade taking into account the Community's present international commitments.* In brief, the applicant submits that the SHD clearly violates first condition of proportionality, which requires a measure be capable of achieving a legitimate public policy objective of the Union.

54. Moreover, recital 56 of Directive 95/46 states that: "*this Directive does not stand in the way of transfers of personal data to third countries which ensure an adequate level of protection*", and that "*the adequacy of the level of protection afforded by a third country must be assessed in the light of all the circumstances surrounding the transfer operation or set of transfer operations*". Those circumstances, of course, include the evidence accepted by the referring court of generalised access by US security authorities to transferred personal data. This access does not require any relationship between the access to the data and a specific concern for and a threat to public security. It does not, therefore, respect the principle of 'purpose limitation' in Article 8(2) CFR. There is no limitation on such generalised access: (i) to data pertaining to a particular time period and/or a particular geographical zone and/or to a circle of particular persons likely to be involved, in one way or another, in a serious

[60] *Digital Rights Ireland*, para 52: where the Court cited, *inter alia*, Case C-473/12 *IPI* EU:C:2013:715, para 39.
[61] *Ibid.*, paras. 47-48.

crime; or (ii) to persons who could, for other reasons, contribute, by the retention of their data, to the prevention, detection or prosecution of serious offences.

55. Thus, the SHD, like the Data Retention Directive considered in ***Digital Rights Ireland***, *"fails"*, by virtue of the letdown of the US law deemed to provide adequate protection in the SHD. The SHD fails *"to lay down any objective criterion by which to determine the limits of the access ... to the data and their subsequent use for the purposes of prevention, detection or criminal prosecutions concerning offences that, in view of the extent and seriousness of the interference with the fundamental rights enshrined in Articles 7 and 8 of the Charter, may be considered to be sufficiently serious to justify such an interference."*[62] It thereby fails to provide for adequate protection

56. The SHD is also inappropriate to pursue its supposed purpose, by comparison to ***Digital Rights Ireland***, because, given the structure of the SHD under which the application of US law is accepted by the Commission, the degree to which the fundamental right of European users of Facebook will be protected depends on the law of a third country that limits, according to a study commissioned by the European Parliament, the protection of the right to privacy under the its own constitutional law to its own citizens and permanent residents.[63] Furthermore, the SHD Decision ignores the fact that not only private activity but also the activity of public authorities may be a source of violation of rights under Articles 7 and 8 CFR. It finds a system to be 'adequate' that allows for transfer of data in absence of substantive and procedural conditions relating to the access by the US security authorities to the transferred data and to their subsequent use thereof under US law. This clearly violates the principles enunciated in ***Digital Rights Ireland*** that objective criteria should be laid down by which the number of persons authorised to access and subsequently use the data retained is limited to what is **strictly necessary** in the light of the objective pursued.[64] Those principles also require that such minimum safeguards be *"specific and adapted to: (i) the vast quantity of data"* which can be transferred; *"(ii) the sensitive nature of that data"*; and *"(iii) the risk of unlawful access to that data, rules which would serve, in particular, to govern the protection and security of the data in question in a clear and strict manner in order to ensure their full integrity and confidentiality"*.[65] The applicant submits that the minimum requirements specified in ***Digital Rights Ireland*** (especially at paragraph 62) are the same as those that should apply in assessing whether adequate protection is afforded by third countries for rights protected under Articles 7 and 8 CFR.

---

[62] *Digital Rights Ireland*, para. 60.

[63] See, for a synopsis of the situation in US constitutional law, Bowden/Bigo, *"The US surveillance programmes and their impact on EU citizens' fundamental rights"*: study requested by the Committee on Civil Liberties, Justice and Home Affairs Committee of the European Parliament, September 2013.

[64] *Digital Rights Ireland*, para. 62.

[65] *Ibid.*, para. 66.

Limitation Strictly Necessary – Availability of Less Onerous Options

57. Limitations to fundamental rights of individuals are only **strictly necessary**, if no measures are conceivable that might limit the relevant fundamental rights to a lesser degree than the ones chosen. It is well established that compliance with the proportionality principle has to be, at least implicitly, explained in the reasoning of an EU act that limits fundamental rights. In this respect too, the SHD violates the principle of proportionality, whilst also suffering from a lack of reasoning under Article 296 TFEU. The reasoning needs to be sufficient to allow the courts to undertake a review of a decision. Thus, the statement of reasons "*must disclose in a clear and unequivocal fashion the reasoning followed by the Community authority which adopted the measure in question in such a way as to make the persons concerned aware of the reasons for the measure and thus enable them to defend their rights and to enable the Court to exercise its supervisory jurisdiction*".[66] Compliance with proportionality – especially showing that the Commission has considered the means which least limits the rights of individuals – has to result from the text of the act and be generally indicated in its preamble.[67] However, the SHD is devoid of consideration as to possible alternatives involving less far-reaching limitations. Equally, no, even implicit, discussion of the consequences of the Decision for the protection of individual rights is offered. Consequently, it breaches the obligation to give sufficient reasons under Article 296 TFEU, and, in so doing, violates the principle of proportionality regarding the 'least-onerous-measure' test; since the Commission failed to indicate why the far-reaching limitations it implicitly endorses of individual privacy rights of the data subjects of European controllers users could be justified as **strictly necessary** to facilitate the free flow of their data to the USA.

58. Indeed, the contrary is in fact the case. In recital 5 to the SHD, the Commission declares itself effectively uncertain as to whether any of limitations under the SHPs are in fact the least onerous possible. Thus, the Commission admits that "*the adequate level of protection for the transfer of data from the Community to the United States recognised by this Decision, **should** be attained if organisations comply with the safe harbour privacy principles...*' (emphasis added). There was therefore merely an aspiration even when the SHD was adopted in July 2000 that the SHPs would actually achieve their objective. In that sense, and independently even of the revelations that have in the meantime emerged of the "*mass and undifferentiated* access" by US security agencies under the 'PRISM' program and the FISA to personal data that are transferred to the USA, the applicant submits that it was clear, even, *ab initio*, that the limitations on the right to privacy of all data subjects whose data would be transferred to the USA, by voluntarily participating and self-certifying organisations to the SHPs like Facebook Ireland, was not **strictly necessary**.[68]

---

[66] Case C-269/90 *Technische Universität München* [1991] ECR I-5469, paras, 14 and 26.
[67] Case T-461/08 *Evropaiki Dynamiki* [2011] ECR II-0000, paras. 118-124.
[68] In fact, the Commission itself has documented violations of rights and other cases of malfunction of the SHD in its three implementing reports in 2002, 2004 and 2013 (see Commission documents SEK(2002) 196 of 13.12.2002 and SEC(2004) 1323 of 20.10.2004 and Commission document COM(2013) 847 final, of 27

59. The applicant submits that many less onerous ways to achieve the public interest in enhancing trade with the United States, which neither require that the applicant's fundamental rights to be rendered unenforceable nor that allow a foreign government to use personal data for mass surveillance, are imaginable. Thus, no adequacy decision could have been adopted, since trade with the US can also be fostered by decisions under Article 25(1) and (2), in combination with, where necessary, Article 26, of Directive 95/46. These provisions generally allow data transfers after individual analysis of adequacy or the application of exceptions listed in Article 26(1). In addition Article 26(2) allows the use of contractual clauses, binding corporate rules (BCRs) or other contractual instruments, e.g. for not strictly necessary but legitimate scenarios like the 'outsourcing' of processing operations to a third country. These instruments are used in relation to all trading partners of the Union, which do not provide 'adequate protection'. The only difference between Article 26 and Article 25(6) is that, under the later, there is a broad adequacy decision which results in an unlimited free flow of data, as occurs within the EEA, while Article 26 requires that one of the many exceptions in Article 26(1) or (2), which are subject to the scrutiny of the DPAs, be fulfilled. Allowing data transfers to the United States under supervision by DPAs and suspension of specific data flows if the fundamental rights of data subjects are, or are likely to be, violated would, thus, have been a far less onerous alternative to the SHD adopted under Article 25(6), which unduly limits the discretion of DPAs to take action if the fundamental rights of data subjects are in fact violated.

60. Another less onerous form of regulation, it is submitted, could have comprised the creation of criteria for the limitation of access by foreign authorities to data transferred from the EU to the US. In ***Digital Rights Ireland*** the Court criticised the Data Retention Directive for failing "*to lay down any objective criterion by which to determine the limits of the access ... to the data and their subsequent use for the purposes of prevention, detection or criminal prosecutions concerning offences that, in view of the extent and seriousness of the interference with the fundamental rights enshrined in Articles 7 and 8 of the Charter, may be considered to be sufficiently serious to justify such an interference.*" The Commission could have introduced exceptions and limitations for excessive access by espionage, national security or law enforcement authorities. It could have achieved this by insisting on an "international commitment" by the US, as it did, e.g., for Passenger Name Records. This would have allowed the Commission to ensure minimal standards of protection and would have allowed it to take factual measures if the USA violated such an agreement

Overall Reasonableness

61. The SHD also fails the overall reasonableness test, *i.e.* the third test of proportionality,

---

November 2013). The November 2013 report is the most damning, insofar as it lists considerable weaknesses of the 'safe harbour' self-certification system and the consequences flowing therefrom for the protection of rights of individuals.

which concerns the overall control of the whether there is a balanced relationship between ends and means. With regard to validity of the SHD, it is the interest in free trade and the free flow of data with the USA that must be balanced with that of the protection of the data subjects' fundamental rights. Yet, the SHPs foresee far-reaching exceptions compared to EU data protection provisions. Potentially any provision of US law, government regulation or court ruling could unilaterally set aside all protection provided by the SHPs. This arises chiefly from the exception created by paragraph 4 of the SHPs in Annex I of the SHD. This results from the functioning of the SHD as a mere EU law 'wrapper', which, by declaring the adequacy of the US rules listed in the annex, aims at formally fulfilling the requirements of Article 25(6) Directive 95/46. Since paragraph 6 of Annex I to the SHD declares US law applicable to the SHPs, the exceptions or limitations on the right to privacy under the SHPs will fall, in principle, to be construed under US law alone. Thus, as a protection for EU citizens, the SHPs are little more than a chimera as regards fulfilling the requirements of Article 25(6) Directive 95/46.

62. However, this Court has consistently held that any acts of the Union institutions must comply with fundamental rights standards established by Union law. In ***Kadi I***, for example, confirmed in ***Kadi II***[69] the Court held that "*respect for human rights is a condition of the lawfulness of Community acts ... and that measures incompatible with respect for human rights are not acceptable in the Community*".[70] Furthermore, it held that no provisions of public international law — and it is submitted that this is all the more true for the law or a self-certification programme of a foreign country — can "*be understood to authorise any derogation from the principles of liberty, democracy and respect for human rights and fundamental freedoms enshrined in Article 6(1) EU as a foundation of the Union*".[71] This reasoning, applied by analogy to this case, requires that the Commission's adequacy decision under Article 25(6) of Directive 95/46 cannot result in data being transferred without further control to a foreign jurisdiction where they are effectively stripped of "*the guarantee of effective judicial protection*" assured by both the CFR and ECHR.[72]

(iii) Invalidity of the SHD for failure to ensure for control by an independent authority

63. In ***Digital Rights Ireland***, the Court held that "*above all*" one of the failings of the Data Retention Directive was that access by the competent national authorities to the data retained was "*not made dependent on a prior review carried out by a court or by an independent administrative body whose decision seeks to limit access to the data*

---

[69] Joined Cases C-584/10P, C-593/10P and C-595/10P *United Kingdom & Others v Kadi* ECLI:EU:C:2013:518, para. 88.
[70] Joined Cases C-402/05 P and C-415/05 P *Kadi and Al Barakaat* [2008] ECR I-6351, para. 284.
[71] *Ibid.*, para. 303.
[72] *Ibid.*, at para. 133 and for the ECHR see ECtHR No 10593/08, judgment of 12 September 2012 in *Nada v Switzerland*, at para. 211.

and their use to what is strictly necessary for the purpose of attaining the objective pursued and which intervenes following a reasoned request of those authorities submitted within the framework of procedures of prevention, detection or criminal prosecutions". In this case, a further clear failing of the SHD is the comparable absence of provisions for control by an independent authority of compliance with the requirements of protection and security of personal data under Article 8(3) CFR. However, this is an express requirement under Article 39 TEU, under which rules adopted by Union institutions regarding the processing or free movement of personal data "*shall be subject*", with regard to compliance, "*to the control of independent authorities*". Furthermore, this requirement is repeated in Article 16(2) TFEU.[73]

64. A definition of an independent supervisory authority is provided in recital 63 of Directive 95/46, which states that supervisory authorities "*must have the necessary means to perform their duties, including powers of investigation and intervention, particularly in cases of complaints from individuals and powers to engage in legal proceedings*". This definition is based on the Council of Europe Convention No. 108 of 1981.[74]

65. This Court has held that the independence of supervisory authorities is an essential component of the right to the protection of personal data. Ironically, this has been confirmed in infringement actions brought by the Commission against Germany and Austria for those Member States' failure to comply with their obligations under Directive 95/46.[75] In its complaint against Germany, the Commission contended that Germany was in breach of its obligations by not giving sufficient independence to its data protection supervisors. The Commission contended that an independent data protection supervisor is essential. The Court agreed. It held that the guarantee of the independence of national supervisory authorities: "*is intended to ensure the effectiveness and reliability of the supervision of compliance with the provisions on protection of individuals with regard to the processing of personal data and must be interpreted in the light of that aim*"; and that: "*It was established not to grant a special status to those authorities themselves as well as their agents, but in order to strengthen the protection of individuals and bodies affected by their decisions*".[76]

66. The applicant submits that SHD manifestly fails to comply with this requirement. Within its annexes provision is made for a rather unique construct comprising essentially two elements: firstly, a voluntary regime of arbitration by private bodies, especially mentioning in FAQ 11 TRUSTe and BBBonline; and, secondly, a possibility of referral of questions from these bodies to the FTC (see FAQ 11 in

[73] The importance of this requirement was stressed by the Court in Case C-614/10 *Commission v Austria* EU:C:2012:631, para. 36.
[74] Additional Protocol to the Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data regarding supervisory authorities and trans-border data flows of 8 November 2001.
[75] Case C-518/07 *Commission v Germany* [2010] ECR I-1885, paras. 23-25, and Case C-614/10 *Commission v Austria* [2012] ECR I-0000, para 37.
[76] Case C-518/05, paras. 23-25 (emphasis added).

Annex 2 to the SHD).[77] The SHPs comprise a code of conduct to which companies can voluntarily subscribe. This is made public by a listing of such companies on a list maintained by the US Department of Commerce.[78] In case of disputes between a self-certified company and a consumer, dispute resolution is undertaken by private arbitrators, such as 'BBBOnline' and 'TRUSTe'. These private arbitration structures may only investigate complaints regarding the private activities of self-certifying companies. It is clear from FAQ 11 that they have no power to review the legality of activity of public authorities within the US. With regard to the FTC, it commits itself under FAQ 11 to reviewing, on a priority basis, referrals received from privacy self-regulatory organizations, such as BBBOnline and TRUSTe, and EU Member States alleging non-compliance with the SHPs and to determine whether section 5 of the FTC Act, which prohibits unfair or deceptive acts or practices in commerce, has been violated.[79]

67. The types of available review are explicitly designed to cover only the activities of undertakings which have self-certified themselves as coming under the SHPs. The FTC appears to have no jurisdiction to review possible violations of data protection principles of public actors, such as the US government or security authorities like the NSA.[80] Yet, this power is essential to guarantee fully effective data protection rights.

68. Accordingly, the Commission could not have found, in adopting the SHD, that, with regard to all the data that would be transferred to the US, there would be adequate protection for the right conferred by Article 8(3) CFR, *i.e.* effective provision for control to be effected by an independent authority of compliance with the requirements of protection and security of personal data.

(iv) Invalidity of the SHD due to incompatibility with the right to an effective remedy in EU law

69. The right to an effective remedy for violation of an EU-law protected right is assured by the CFR (especially Article 47) and by the general principles of Union law[81] (*ubi*

---

[77] Other bodies offering such arbitration under the SHPs include the 'Direct Marketing Association Safe Harbour Programme', the 'Entertainment Software Rating Board Privacy Online EU Safe Harbour Programme', the 'Judicial Arbitration and Mediation Service (JAMS)' and the 'American Arbitration Association'.

[78] This list, however, is far from regularly updated and may contain companies which are no longer compliant with the voluntary code of conduct, or which have, despite self-certification, never fully complied. See the report of the German Federal Agency for Data Protection and Access to Information: Deutscher Bundesbeauftragter für den Datenschutz und die Informationsfreiheit at http://www.bfdi.bund.de/DE/EuropaUndInternationales/Art29Gruppe/Artikel/SafeHarbor.html?nn=409532.

[79] The FTC does not generally investigate complaints from data subjects like the applicant. It has no direct enforcement remedy but may merely find a violation of the SHP also violates s. 5 of the FTC Act.

[80] The applicant made a complaint to the FTC regarding the potential accessing of his personal data, as transferred to the USA by Facebook Ireland, by US security authorities; see Annex A.3.. He has not yet received a response to this complaint.

[81] The Court has repeatedly found this right to be a fundamental right of individuals resulting from the common constitutional traditions of the Member States and recognised by Articles 6 and 13 of the ECHR. The fundamental rights arising from this are thus also protected as general principles of EU law under what is now

ius ibi remedium).[82] It requires an effective remedy before a court to seek to challenge measures that restrict the right to privacy and the protection of one's personal data.

70. With regard to data protection, the applicant submits this means that persons whose data has been accessed or subject to surveillance measures need to be informed about this. This is a pre-condition for the possibility to exercise the right to an effective remedy. In ***Weber and Saravia v. Germany***, the ECtHR explicitly recognised the importance of a notification in the context of surveillance measures, because it permits the individuals affected to be informed and, if they wish, more effectively to challenge the legality of such surveillance measures, *i.e.* effectively to exercise a remedy against such measures.[83] This Court has upheld in ***Digital Rights Ireland*** the importance of information as the minimum safeguard required to counter the concern of constant surveillance.[84]

71. The applicant submits that the SHD violates the right to an effective judicial remedy, because it allows for no effective *de jure* or *de facto* remedies against violation of the right to the protection of personal data where such data are transferred to the USA. Under the SHD, there is neither a possibility within the EU effectively to challenge violations to the rights to privacy and data protection following the transfer of data to the USA, nor is there one in the US legal system.[85] There is no point to having high levels of data protection within the EU if data that would be protected within the EU against indiscriminate access and retention may be transferred to a third country that quite plainly does not apply the same standard. Such 'digital refoulement' would, the applicant submits, be the very antithesis of the effective protection of personal data that is guaranteed by the CFR and by the general principles if Union law.

72. The SHD deprives EU citizens and residents, as consumers of companies who transfer their personal data to the US, of an effective right to seek judicial review of the violation of their rights. It manifestly fails to provide, by any benchmark, an adequate standard of protection compared to that which applies within the EU, both under Article 47 CFR and the general principles of Union law, as well as under Directive

---

Article 6(3) TEU by the Court's consistent case-law: see, e.g.: Case 222/84 *Johnston* [1986] ECR 1651, paras 18 and 19; Case 222/86 *Heylens and Others* [1987] ECR 4097, para 14; Case C-50/00 P *Unión de Pequeños Agricultores v Council* [2002] ECR I-6677, para 39;; Case C-432/05 *Unibet* [2007] ECR I-2271, para 37; Joined Cases C-402/05 P and C-415/05 P *Kadi and Al Barakaat* [2008] ECR I-6351, para 335; and Joined Cases C-317/08 to C-320/08 *Alassini* [2010] ECR I-2213, para 61.

[82] The remedy must be available, by analogy to Article 13 ECHR, upon an "*arguable claim of violation*", and must be effective both in law and in practice: ECtHR Applications Nos. 5947/72; 6205/73; 7052/75; 7061/75; 7107/75; 7113/75; 7136/75 *Silver and Others* §113 ECHR 1975 and Application No 30210/96 *Kudla v Poland* [GC] §157, ECHR 2000-XI.

[83] No. 54934/00 of 29 June 2006.

[84] Para. 37. See also Boehm/de Hert, "Notification, an important safeguard against the improper use of surveillance – finally recognized in case law and EU law", European Journal of Law and Technology, Vol. 3, No. 3, 2012.

[85] TRUSTe, the FTC and US courts lack jurisdiction to find that the SHPs could overrule the FISA . As a non-US person, the applicant also has no right to challenge the FISA. Finally, the DPC refused to investigate the legality of the transfer from the Ireland to the USA.

95/46 and in particular Article 22 thereof, whereunder every person adversely affected by data processing is granted the right to apply for judicial remedies. Instead, under the SHPs (FAQ 11) data subjects are supposed to contact the abovementioned dispute resolution bodies. These bodies are not organised uniformly and establish their own procedural rules. Individuals within the EU can turn to a US-based specialised arbitration entity like TRUSTe or BBBonline to seek clarification whether the company who holds their personal data of EU citizens in the US is violating the terms of the self-certification regime. However, this system of arbitration cannot qualify as an equivalent to an effective judicial review. Private arbitration by bodies such as TRUSTe cannot address violations of the right to the protection of personal data by bodies other than the self-certifying companies. Critically they lack competence to rule on the legality of US governmental agencies' activities. Moreover, such bodies have wide discretion in decision-making and in the selection of remedies but there is no indication within the SHPs that such decisions may then be contested before a court. Thus, data subjects may be cut off from judicial remedies by a decision of such a dispute resolution body.[86]

73. The SHD is thus incompatible with the right to an effective remedy in EU law.

74. This conclusion is reinforced also by the SHPs being based on an approach to dispute settlement which promotes 'unfair' terms under EU consumer protection law contrary to Article 6(1) to Council Directive 93/13/EEC of 5 April 1993 on unfair terms in consumer contracts. Under Directive 93/13 arbitration clauses putting consumers at a disadvantage in the protection of their rights are not binding on them.[87] Amongst the indicative list of unfair terms included in the Annex to Directive 93/13 (at paragraph 1(q)) are terms having the object or effect of "*excluding or hindering the consumer's right to take legal action or exercise any other legal remedy, particularly by requiring the consumer to take disputes exclusively to arbitration not covered by legal provisions, unduly restricting the evidence available to him or imposing on him a burden of proof which, according to the applicable law, should lie with another party to the contract*". Under the SHPs, consumer complaints fall to be determined by private arbitration bodies. Thus, in the main proceedings, the SHPs are based on the understanding that the applicant, an EU national and resident consumer, is supposed to enter into a contract with Facebook Ireland, an EU registered company, for the provision of social media services to be provided within the EU on his internet-devices, such as his phone and computer that is governed as to the critically important

[86] Thus, if self-certified 'safe harbor' organisations like Facebook USA fail to comply with the rulings of such bodies, the latter must notify the governmental body with applicable jurisdiction, such as the FTC, who may then seek a court order by filing a complaint in a federal district court. However, it is not obliged to do so and may choose instead to seek an administrative 'cease and desist' order against the organisation. Moreover, the FTC considers itself entitled only to investigate matters falling within s. 5 of the FTC Act, which prohibits unfair or deceptive acts or practices in commerce, a prohibition which would not appear to cover the control of the legality even of "*mass and undifferentiated*" access by US security authorities to the personal data of EU citizens based on US legislation.

[87] OJ (1993) L 95, p. 29.

issue of the protection of the privacy of his data by the law of a third country, to wit the USA, with which he has no connections. It is difficult to conceive of a more unfair term from a European consumer's perspective.

75. Furthermore, for the consumer Facebook user to 'benefit' from the 'safe harbor' regime with regard to the protection of his personal data, which is transferred to the USA by Facebook Ireland, s/he must agree to settle disputes regarding issues arising with regard to that protection in the USA with a US company (Facebook USA) s/he has no direct contractual relation with, by a US based arbitration company, TRUSTe, which is undertaken in the US and under US law. Thus, practically an entirely EU-focused and located transaction is submitted to the law and the dispute-settlement mechanisms of a third country, in a language (English) which for most EU consumers (including the applicant) is not their mother tongue, and at a place which it would be prohibitively expensive for many to reach. It is, therefore, hardly surprising that the applicant understands that the arbitration mechanisms have in the past 14 years rarely been used by EU nationals affected by data transfers to the US of their personal data. In ***Asturcom v Nogueira,***[88] a case regarding the legality of an arbitration clause in a consumer contract, this Court held that, a national court confronted with such an arbitration clause is "*obliged to assess of its own motion whether that clause is unfair*" in the light of Article 6 of Directive 93/13.[89] The applicant submits that that the SHPs impose grossly unfair terms of contract on consumers with regard to disputes arising from the processing of their personal data. This is incompatible with the requirement to ensure effective judicial protection under Article 47 CFR.

C. Obligation of the DPC to take appropriate action

76. By its second question, the referring court has asked if the DPC "*may and/or must*" conduct its own investigation in the light of the factual developments of EU law. The applicant submits that an answer to this question should be given irrespective of whether the Court invalidates the SHD or interprets the SHD in a way compatible with the fundamental rights under EU law. Member State institutions, bodies and agencies, are obliged when implementing EU law or acting within its scope, to comply in their actions with fundamental rights and other general principles of EU law.[90] This is also explicitly prescribed in Article 51 CFR.[91] The legality of action of a Member State authority like the DPC is therefore subject not only to national law but also to compliance with general principles of EU law, including the protection of fundamental rights. When the DPC is called upon by a complainant to decide about the legality of the transfer of personal data to third, non-EEA countries, it implements

[88] Case C-40/08 [2009] ECR I-9579, para. 29.
[89] See Case C 168/05 *Mostaza Claro* [2006] ECR I-10421, para. 38, and *Asturcom v Nogueira,* loc. cit., paras. 53-54.
[90] Case C-260/89 *ERT* [1991] ECR I-2925, para 42; Case C-617/10 *Åkerberg* ECLI:EU:C:2013:105,paras 20-27.
[91] As interpreted in, e.g., Case C-617/10 Åkerberg, paras 20-27 together with further references.

the provisions of Article 25 and 26 Directive 95/46 under the relevant provisions of the 1998 Irish Act, as amended, that implements the Directive in Ireland. Directive 95/46 is itself, as discussed above, a concretisation of the right to privacy and data protection guaranteed by the general principles of EU law and under Articles 7 and 8 CFR. Given that these provisions correspond to Article 8 ECHR, their meaning and scope, under Article 52(3) CFR, falls to be interpreted in the same way. The ECtHR has held consistently that Article 8 ECHR requires: *"not only that the State refrain from interfering with private life but also entail certain positive obligations on the State to ensure effective enjoyment of this right by those within its jurisdiction."*[92] It is firmly established that these fundamental rights place a duty on Member States and the Union reasonably to protect them against violations by third parties. Furthermore, Article 47 CFR gives the applicant a right to an effective remedy and a fair trial. Thus, the DPC is obliged to conduct an investigation under the general principles of EU law, since no other possibility exists of investigating whether 'effective enjoyment of' his rights is ensured. In light of the duties of the DPC to protect the fundamental rights of the applicant, he submits that the DPC has an active duty to not only investigate, but, if the complaint is upheld, to use its powers to suspend data flows between Facebook Ireland and Facebook USA in accordance with the law.

IV. CONCLUSION

77. Accordingly, the applicant respectfully proposes to the Court of Justice that it answer the within questions referred to it by the High Court of Ireland as follows:

1) A competent national data protection supervisory authority, such as the DPC in the main proceedings, is not bound by the finding of adequacy of protection with regard to US laws and practices contained in Commission Decision 2000/520 by reason of the incompatibility of the latter with Directive 95/46/EC, and Article 25(6) thereof in particular, construed in the light of the requirements of Articles 7, 8 and 47 CFR, as well as Articles 39 TEU and 16 TFEU;

2) Articles 7, 8 and 47 CFR, as well as Articles 39 TEU and 16 TFEU, place a positive obligation on national supervisory authorities to ensure effective enjoyment of the rights guaranteed by Directive 95/46, and, consequently, they must investigate arguable complaints made to them regarding infringements of the right to privacy and data protection, such as a complaint regarding mass and undifferentiated access to data transferred to a third country.

Paul O'Shea, Barrister,
Professor Herwig Hofmann, Rechtsanwalt,
Noel J. Travers, Senior Counsel.

---

[92] See *Mosley v. United Kingdom*, 10 May 2011, [2011] ECHR 774, with further references.

Original dated this 10th day of November 2014:

Signed: [redacted]

Gerard Rudden, Solicitor,
Ahern Rudden Solicitors,
Solicitors for the Applicant,
5 Clare Street,
Dublin 2,
Ireland.

LIST OF ANNEXES

Annex A.1: 'Opinion on the adequacy of the Safe Harbor Decision', Prof. Dr. Franziska Böhm, University of Münster (Germany);

Annex A.2: Complaint by Max Schrems to TRUSTe and response of TRUSTe;

Annex A.3: Complaint by Max Schrems to the US Federal Trade Commission (to date unanswered);

Annex A.4: List of FTC Decisions in the context of 'Safe Harbor Matters' to date (format Excel).

Date de réception : 23/01/2015

WE HEREBY CERTIFY THE WITHIN TO BE TRUE COPY OF THE ORIGINAL

[redacted]

GERARD RUDDEN
SOLICITOR
5 CLARE ST.
DUBLIN 2

CASE C-362/14

MAXIMILLIAN SCHREMS

Applicant

V.

DATA PROTECTION COMMISSIONER

Respondent

AND

DIGITAL RIGHTS IRELAND LIMITED

Amicus curiae

Annex A.1

Opinion on the adequacy of the Safe Harbor Decision, Prof. Dr. Franziska Böhm

WESTFÄLISCHE
WILHELMS-UNIVERSITÄT
MÜNSTER

WESTFÄLISCHE WILHELMS-UNIVERSITÄT

Institute for Information-, Telecommunication- and Media-Law (ITM)

Prof. Dr. Franziska Boehm

Assistant Professor for IT-Law

Opinion on the adequacy of the Safe Harbor Decision

November 9
2014

Comparison between Safe Harbor and Directive 95/46

Content

Abbreviations used in the opinion

CFR = Charter of Fundamental Rights of the European Union

Communication of the Commission on the functioning of SH =

Communication from the Commission to the European Parliament and the Council on the functioning of the Safe Harbour from the Perspective of EU Citizens and Companies Established in the EU of 27th of November 2013, Com(2013) 847

Directive 95/46 = Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data, OJ 1995, L 281/31

ECHR = European Convention on Human Rights

ECtHR = European Court of Human Rights

SH = Safe Harbor

SHD = Commission Decision of 26 July 2000 pursuant to Directive 95/46/EC of the European Parliament and of the Council on the adequacy of the protection provided by the safe harbour privacy principles and related frequently asked questions issued by the US Department of Commerce, OJ 2000, L 215/7

US = United States

Other abbreviations relating to specific measures are explained in the text.

The opinion includes a brief comparison between the basic data protection guarantees of Directive 95/46 and the guarantees stipulated by the Safe Harbor Decision (SHD in the following). It should give a quick overview of the most important data protection principles in both instruments and serve as background information for the written observations.

Starting point for the opinion are the provisions of Directive 95/46 allowing the transfer of personal data of EU citizens to a third state. For this purpose, Article 25 (1) of Directive 95/46 requires an adequate level of protection in the third country. The directive does not require an equivalent level of protection, meaning that the guarantees in the third country can differ from the data protection guarantees in the EU to a certain degree. The difference in the wording leaves a certain leeway for the Commission to accept an adequate level of protection in a third country although the data protection guarantees in the third country do not meet exactly the same level as those in the EU. Nonetheless, it is clear that the adequacy decision of the Commission requires the respect of basic data protection guarantees.

When assessing the adequacy, the following criteria stipulated in Article 25 (2) of Directive 95/46 play a role: "the circumstances surrounding a data transfer operation or set of data transfer operations; the nature of the data, the purpose and duration of the proposed processing operation or operations, the country of origin and country of final destination, the rules of law, both general and sectoral, in force in the third country in question and the professional rules and security measures which are complied with in that country".

It results from the wording of Article 25 (1) and (2) that they are designed to enable adequacy decisions for entire countries. However, as the data protection framework in the US as an entire country could not be assessed as adequate, a specific regime, the SHD, was put in place to enable data transfer in specific situations. This special legal nature of the SHD leaves however no doubt on the general applicability of basic data protection principles.

The following analysis is not intended to be exhaustive. It focuses on a comparison of the most important EU data protection principles that are illustrated by means of comparative tables.

I. APPLICATION OF SAFE HARBOR

1. Scope

a) General Remarks

Directive 95/46 has a broad application to all private and public "controllers" of personal data within the EU. Only activities that fall outside of the scope of Community Law (e.g. states security, law enforcement and defence) are not governed by Directive 95/46 under Article 3, but will usually be governed by the ECHR, CFR and/or national constitutional laws of the EU member states.

In contrast to the wide application of Directive 95/46, the self-certification system of Safe Harbor (SH in the following) only applies to certified organizations established in the United States. This means that contrary to Directive 95/46, all government authorities and all non-certified organizations in the United States are outside of the SH system. As soon as data is transferred to a non-certified entity, the SH rules do not apply anymore (see "transfer" below).

Directive 95/46	Safe Harbor
Article 3 Scope 1. This Directive shall apply to the processing of personal data wholly or partly by automatic means, and to the processing otherwise than by automatic means of personal data which form part of a filing system or are intended to form part of a filing system. 2. This Directive shall not apply to the processing of personal data: - in the course of an activity which falls outside the scope of Community law, such as those provided for by Titles V and VI of the Treaty on European Union and in any case to processing operations concerning public security, defence, State security (including the economic well-being of the State when the processing operation relates to State security matters) and the activities of the State in areas of criminal law, [...] *[See also Articles 1, 2 and 4 of Directive 95/46 for the application of the Directive.]*	**Third Paragraph** Decisions by organizations to qualify for the safe harbor are entirely voluntary, and organizations may qualify for the safe harbor in different ways. [...] **Fifth Paragraph** Organizations may wish for practical or other reasons to apply the Principles to all their data processing operations, but they are only obligated to apply them to data transferred after they enter the safe harbor. [...]

b) Result of Comparison

While Directive 95/46 generally applies to a range of private and public processing operations in the EU/EEA, the SH rules only apply to the US entities that have self-certified. Currently, the list includes more than 3800 companies. As the self-certification mechanism is not designed for the public sector, government authorities are not on the SH list. In this context, it should be briefly mentioned that SH is the first instrument with which a "sectoral self-certification" mechanism is found to be adequate. This can conflict with Article 25 Directive 95/46, which wording refers to a (whole) country (not a certificate)

to be found "adequate". The only other existing adequacy decision referring to only one specific sector of a country is a second US-related decision, concerning the transfer of flight passenger data.[1]

Further, if SH data is transferred to a public or private entity under a legal obligation or else resulting from US law, there is no subsequent protection following from the SH mechanism. While in the EU, individuals concerned by data processing operations are not only protected by the regime of Directive 95/46, but also by human rights and/or constitutional protection, if data is transferred outside of the scope of Directive 95/46, there is almost no protection available in the US for EU data that have been transferred to the US under the SH regime and that are then transferred to an organization not participating in the SH mechanism. Constitutional protection and protection according to the US privacy act of 1974 are only available to "US persons" (US citizens and legal permanent residence) in the United States.[2]

2. Applicable Law

a) General Remarks

Directive 95/46 is to be interpreted within EU law and primary legislation, such as Articles 7 and 8 CFR and Article 8 ECHR.

Following the system of US self-certification, the SH principles and Frequently Asked Questions are governed and interpreted under US law. In consequence, in cases of doubts relating to the interpretation and applicability of data protection principles in the framework of SH, only US law applies. Only if a US organization has submitted itself to the jurisdiction of a European Data Protection Authority, its data processing activities are to be interpreted under EU law.

Directive 95/46	Safe Harbor
Article 4, National law applicable 1. Each Member State shall apply the national provisions it adopts pursuant to this Directive to the processing of personal data where: (a) the processing is carried out in the context of the activities of an establishment of the controller on the territory of the	**Sixth Paragraph** U.S. law will apply to questions of interpretation and compliance with the Safe Harbor Principles (including the Frequently Asked Questions) and relevant privacy policies by safe harbor organizations, except where organizations have committed to cooperate with European Data Protection

[1] Compare overview of the adequacy decisions: http://ec.europa.eu/justice/data-protection/document/international-transfers/adequacy/index_en.htm#h2-12.

[2] Compare for instance: Bowden, "The US surveillance programmes and their impact on EU citizens' fundamental rights" study requested by the European Parliament's Committee on Civil Liberties, Justice and Home Affairs in September 2013, p. 20, para 2.2.3, available at: http://www.europarl.europa.eu/RegData/etudes/note/join/2013/474405/IPOL-LIBE_NT%282013%29474405_EN.pdf and Privacy Act of 1974 (Pub.L. 93–579, 88 Stat. 1896, enacted December 31, 1974, 5 U.S.C. § 552a) together with the proposal to extend the privacy protections of the Privacy Act of 1974 to non-U.S. Persons in the recent report of the executive office of the president, "Big Data: seizing opportunities, preserving values" of May 2014, p. 60, available at: http://www.whitehouse.gov/sites/default/files/docs/big_data_privacy_report_may_1_2014.pdf.

Member State; when the same controller is established on the territory of several Member States, he must take the necessary measures to ensure that each of these establishments complies with the obligations laid down by the national law applicable; (b) the controller is not established on the Member State's territory, but in a place where its national law applies by virtue of international public law; (c) the controller is not established on Community territory and, for purposes of processing personal data makes use of equipment, automated or otherwise, situated on the territory of the said Member State, unless such equipment is used only for purposes of transit through the territory of the Community. 2. In the circumstances referred to in paragraph 1 (c), the controller must designate a representative established in the territory of that Member State, without prejudice to legal actions which could be initiated against the controller himself.	Authorities. Unless otherwise stated, all provisions of the Safe Harbor Principles and Frequently asked Questions apply where they are relevant.

b) Result of Comparison

While Directive 95/46 must be interpreted in line with higher ranking law (e.g. the CFR and the ECHR)[3], the SH is subject to US interpretation, US laws and the US constitution, which are not granting privacy protection for "non-US persons".[4] For instance, the protection of the guarantees resulting from the 4th Amendment to the US Constitution is limited to US citizens.[5] This leads to a very limited privacy protection of EU citizens in the US, even if data are transferred in the framework of SH.

3. Exceptions and Restrictions

a) General Remarks

Article 13 of Directive 95/46 includes a number of limitations and restrictions to the application of five Articles of the Directive. Such limitations are usually to be interpreted narrowly and limited by national constitutional laws, the ECHR and the CFR.[6] SH includes the same limitations and restrictions by referring to Directive 95/46 in subparagraph (c) of the fourth paragraph of the SHD. EU law requires that such restrictions are provided for by a law that fulfils certain minimum requirements, such as accessibility,

[3] Compare Boehm/Cole, Data Retention after the Judgement of the Court of Justice of the European Union, p. 23 et seq., available at: http://www.uni-muenster.de/Jura.itm/hoeren/materialien/boehm/Boehm_Cole-Data_Retention_Study-June_2014.pdf.

[4] Bowden, The US surveillance programmes and their impact on EU citizens' fundamental rights, p. 19.

[5] Bowden, The US surveillance programmes and their impact on EU citizens' fundamental rights, p. 20.

[6] Brühann, in: Grabitz/Hilf, Das Recht der Europäischen Union, 40. Auflage 2009, Sekundärrecht, Teil A 30, Kapitel II, Abschn. VI, Art. 13, Rn. 1. Compare: ECtHR, Rotaru v. Romania, no. 28341/95, para. 47; CJEU, C-293/12 Digital Rights Ireland and 594/12 Seitlinger and Others.

foreseeability and clear and precise rules with regard to the circumstances justifying a limitation.[7] Article 52 (1) of the CFR further requires that limitations and restrictions to the fundamental rights of the CFR respect the essence of the rights and are subject to the principle of proportionality. Further, "limitations may be made to those rights and freedoms only if they are necessary and genuinely meet objectives of general interest recognized by the Union or the need to protect the rights and freedoms of others."[8]

In addition to the limitations that exist in Directive 95/46, the SH adds further exceptions in its fourth paragraph, subparagraphs (a) and (b). The limitation clarifies that any law, government regulation and case law override the self-certification mechanism. In addition all national security, public interest and law enforcement requirements make the SH non-applicable, even if they are not specified in a law, government regulation or case law. The US understanding of this exception is further explained in Annex IV of the SHD, which states that not only a duty to provide data, but also a "special authorization", for instance, to share data, overrides the SH principles. This means in practice that any form of US statute/executive regulation can add further limitations to the ones provided for in Directive 95/46. In consequence, SH principles only apply when there is no other specific regulation within the US legal system.

Directive 95/46	Safe Harbor
Article 13, Exemptions and Restrictions 1. Member States may adopt legislative measures to restrict the scope of the obligations and rights provided for in Articles 6 (1), 10, 11 (1), 12 and 21 when such a restriction constitutes a necessary measures to safeguard: (a) national security; (b) defence; (c) public security; (d) the prevention, investigation, detection and prosecution of criminal offences, or of breaches of ethics for regulated professions; (e) an important economic or financial interest of a Member State or of the European Union, including monetary, budgetary and taxation matters; (f) a monitoring, inspection or regulatory function connected, even occasionally, with the exercise of official authority in cases referred to in (c), (d) and (e); (g) the protection of the data subject or of the rights and freedoms of others.	**Fourth Paragraph** Adherence to these Principles may be limited: (a) to the extent necessary to meet national security, public interest, or law enforcement requirements; (b) by statute, government regulation, or case law that create conflicting obligations or explicit authorizations, provided that, in exercising any such authorization, an organization can demonstrate that its non-compliance with the Principles is limited to the extent necessary to meet the overriding legitimate interests furthered by such authorization; or (c) if the effect of the Directive of Member State law is to allow exceptions or derogations, provided such exceptions or derogations are applied in comparable contexts. **ANNEX IV** **B. Explicit Legal Authorizations** [...]Clearly, where U.S. law imposes a conflicting obligation, U.S. organizations whether in the safe harbor or not must comply with the law. As for explicit authorizations, while the safe harbor principles are intended to bridge the differences between the U.S. and European regimes for privacy protection, we owe deference to the legislative prerogatives of our elected lawmakers. [...] The exception is limited to cases where there is an explicit authorization. Therefore, as a threshold matter, the relevant

[7] ECtHR, S. and Marper v. UK, no. 30562/04 and 30566/04, para. 95; Copland v. UK, no. 62617/00, para. 46; Amann v. Switzerland, no. 27798/95, para. 55.

[8] CJEU, C-293/12 Digital Rights Ireland and 594/12 Seitlinger and Others, para. 38; Compare Boehm/Cole, Data Retention after the Judgement of the Court of Justice of the European Union, p. 34.

	statute, regulation or court decision must affirmatively authorize the particular conduct by safe harbor organizations.

b) Result of Comparison

The US constitution as well as most US laws and regulations do not grant a right to privacy to "non-US persons". In contrast, it is clear from the wording of Annex IV of the SHD that every rule in form of "explicit legal authorizations" (from the federal, state or even the local level) existing in the US can override the guarantees of the SHD. As a result, in particular the provisions of Annex IV are capable of broadly restricting the rights of the persons whose data have been transferred.
In addition to Annex IV there is an exception for "national security", "law enforcement" and "public interest". It is not clear from the wording of this exception whether these restrictions require any basis in a law or regulation. This could mean that even a local town ordinance in the US can override SH. In essence, it is highly likely that SH principles are only applicable in a small number of situations. If however, the SH principles are not applicable, there is no chance of balancing the conflicting interests, as it would be required by EU law, if fundamental rights are restricted.[9] An example is the current situation regarding the "PRISM" program: The FISA Act (50 U.S.C. Chapter 36, § 1801 et seq.) is overriding the SH rules and leaves non-US data subjects with no protection against mass surveillance by US espionage, national security and law enforcement authorities.[10]

In summary, in particular Annex IV of the SHD allows for restrictions and limitations of the fundamental rights of EU citizens which go far beyond of what is tolerated in the EU. The restrictions that are possible according to the SHD decision do not even require a proportionality or balancing test between the different interests at stake. This constitutes a clear violation of Article 7, 8 and 52 (1) CFR and the ECHR and can therefore not be regarded as adequate.

4. Summary Application

With regard to the scope of protection, it can be concluded that the scope of SH is very narrow and includes only the about 3.800 organizations that have "self-certified". If SH data is transferred to organizations which are not subject to the SH rules, constitutional protection or protection following from other legal sources for data of EU citizens is almost non-existent. Privacy and data protection rules in the US differ significantly from the protection guaranteed in the EU. There are no general privacy or data protection laws in the US and constitutional protection of privacy for "non-US persons" is not provided for. Sectoral regulations govern certain aspects of privacy and data protection in a particular context (for instance Health Data, Online Data of Children, Credit Information).

In consequence, protection resulting from US laws and regulations is often weaker than in the EU, in particular for EU citizens. An example is the FISA Act (e.g. 50 U.S.C. Chapter 36, § 1881a) which only

[9] See for example Article 52(1) CFR; Compare Boehm/Cole, Data Retention after the Judgement of the Court of Justice of the European Union, p. 34 et seq.

[10] Bowden, The US surveillance programmes and their impact on EU citizens' fundamental rights, p. 19 et seq.

grants US citizens and permanent residents protection but not EU citizens.[11] The difference regarding the standard of protection is also the reason why the US as a country is not qualified as a country providing "adequate protection" in the sense of Directive 95/46. In summary, the SH rules enable a wide ranging use of data outside the "sphere of protection" of SH. Circumventing the SH principles by transferring SH data to government authorities or other third parties – where lower data protection principles apply (if at all) – is easily possible. This clearly contradicts to EU data protection principles according to which strict data protection rules apply during the entire course of data processing.[12] It is therefore extremely doubtful whether the current SH mechanism can be regarded as providing an adequate protection.

In addition to the week protection outside of the SH framework, the SH rules do not apply if there is US law overriding the application of the SH principles. This US law can include federal, state and local laws, case-law, regulations and even public interests that need no legal specification. Other explicit "authorizations" may even limit the scope further. Moreover, the rules of SH are subject to US interpretation. This weakens the standard of protection for SH data even more, since US privacy and data protection standards differ to a great extend from those of the EU (compare above).

II. SUBSTANTIVE LAW GUARANTEES

1. Data Quality

a) General Remarks

According to EU law "data quality" requirements constitute a central limitation for every kind of data usage.[13] Directive 95/46 requires in its Article 6 the adherence to several principles when it comes to data processing. First, the processing must be fair and lawful. Secondly, according to the purpose limitation principle the collection of data may only take place for specified, explicit and legitimate purposes and further processing, incompatible to those purposes, is prohibited. Thirdly, the (limited) purpose requires that data processing must be adequate, relevant and not excessive. Accuracy and correctness of data is also required, which means that there have to be certain safeguards to get inaccurate or incomplete data erased or rectified. Finally, Directive 95/46 contains a limitation which concerns the extent of the data and demands that data is kept in a form which permits identification of data subjects for no longer than necessary. Each of the principles is not only important as a single principle; they also have a considerable meaning in their entirety. The more general idea of data minimization can be derived from them.[14]

---

[11] Ibid.

[12] Compare CJEU, C-293/12 Digital Rights Ireland and 594/12 Seitlinger and Others, paras. 32, 35.

[13] Compare Handbook on European data protection law, chapter 3 (http://www.echr.coe.int/Documents/Handbook_data_protection_ENG.pdf); Brühann, in: Grabitz/Hilf, Art. 6 Rn. 6.

[14] Compare for instance, European Data Protection Supervisor, https://secure.edps.europa.eu/EDPSWEB/edps/lang/en/EDPS/Dataprotection/Glossary/pid/74.

This idea as well as the specific principles that limit data processing can be found in primary EU law. Article 8 (2) CFR reiterates largely the rules laid down in Article 6 of Directive 95/46.[15] Article 8 ECHR and the case law of the ECtHR with regard to this article regularly refer to the above-mentioned quality requirements.[16] The same principles can be found in the "OECD Guidelines on the Protection of Privacy and Transborder Flows of Personal Data"[17] and the "Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data"[18] of the Council of Europe. The mentioning of these principles in several sources of law and the reference in case law show their high acceptance even beyond mere EU law.

Data quality principles, respectively "data integrity" principles, are laid down in the SHD as well. The purpose limitation principle constitutes the core part. Besides, to ensure reliability of data, the SHD requires accurateness, completeness and correctness of data. The access principle refers to these safeguards.

Directive 95/46	Safe Harbor
Article 6, PRINCIPLES RELATING TO DATA QUALITY 1. Member States shall provide that personal data must be: (a) processed fairly and lawfully; (b) collected for specified, explicit and legitimate purposes and not further processed in a way incompatible with those purposes. [...] (c) adequate, relevant and not excessive in relation to the purposes for which they are collected and/or further processed; (d) accurate and, where necessary, kept up to date; every reasonable step must be taken to ensure that data which are inaccurate or incomplete, having regard to the purposes for which they were collected or for which they are further processed, are erased or rectified; (e) kept in a form which permits identification of data subjects for no longer than is necessary for the purposes for which the data were collected or for which they are further processed. [...]	**DATA INTEGRITY** Consistent with the Principles, personal information must be relevant for the purposes for which it is to be used. An organization may not process personal information in a way that is incompatible with the purposes for which it has been collected or subsequently authorized by the individual. To the extent necessary for those purposes, an organization should take reasonable steps to ensure that data is reliable for its intended use, accurate, complete, and current. **ACCESS** Individuals must have access to personal information about them that an organization holds and be able to correct, amend, or delete that information where it is inaccurate, [...]

[15] Bernsdorff, in: Meyer, Charta der Grundrechte, Art. 8 Rn. 22.

[16] Compare ECtHR, S. and Marper v. UK, no. 30562/04 and 30566/04, para. 103; Gardel v. France, no. 16428/05, para. 62.

[17] Available at: http://www.oecd.org/internet/ieconomy/oecdguidelinesontheprotectionofprivacyandtransborderflowsofpersonaldata.htm#part2.

[18] Available at: http://conventions.coe.int/Treaty/en/Treaties/html/108.htm.

b) Result of Comparison

The SHD mentions data quality requirements. However, crucial elements like "fairness" and "lawfulness" are missing. Since the element of "adequacy" is not mentioned in SH, there is no starting-point for conducting the proportionality test which is crucial in European data protection legislation.[19]

At a first glance the important minimum standard of purpose limitation is contained in the SHD. Nevertheless, the standard is formulated more generously. The SHD does not require the purpose to be "explicit", "specified" or "legitimate". This leads to the assumption that the principle can be easily circumvented. As the further elements (incompatibility; accuracy; completeness; currentness) refer to the defined purpose, the formulation of a broad purpose paves the way for various forms of processing. With regard to such broad definition of the purpose it is not unlikely that the data are regarded as relevant, necessary, compatible and current for various different purposes.

Concerning the concept of data minimization severe doubts arise if the SHD adheres to this principle. The SHD does not explicitly lay down that data must be "not excessive". Additionally, the SHD lacks the clear order to retain data in a form which permits identification of data subjects only as long as it is necessary for the purposes.

All in all it can be observed that the SHD is differing in essential points from European data protection standards. Important minimum standards (fairness, lawfulness, adequacy, explicit purpose limitation) resulting from Directive 95/46, Article 7, 8 CFR and Article 8 ECHR are not applied at all or applied in a less stringent way.

2. Legitimate Processing

a) General Remarks

EU law prohibits data processing, unless there is an explicit allowance. This principle is – next to the data quality principles – the second main limitation on data usage. The general approach was already established in the ECHR. According to Article 8 (2) ECHR the basic requirement for the justification of an interference with the right of private and family life is the existence of a legal basis. Similarly, Article 8 CFR requires permission for every form of data processing operation as well. Directive 95/46 implements the principle by explicitly listing in Article 7 exceptional circumstances in which data processing is not prohibited.

The most relevant condition that makes data processing legitimate is the consent of the data subject. Additionally, the list contains five more reasons that can be applied for arguing that the processing operation is in conformity with data protection law. It is noteworthy that every option contains the word "necessary". This leaves open the possibility to interpret the exceptions narrowly, which is in line with the general approach in EU law to which exceptions should not be interpreted too extensively.

[19] Compare Article 29 Data Protection Working Party, 536/14/EN, available at: http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2014/wp211_en.pdf.

The SH does not know such a general limitation. Instead processing depends only on the application of the notice and choice principles. First, it is required to inform data subjects about the purposes for which data are collected and it is required to give certain additional information. Secondly, the choice principle necessitates the possibility to "opt out" (equivalent to the "right to object" in Article 14 of Directive 95/46) from data processing. But this possibility is limited to two specific situations, which are (a) disclosure to a third party and (b) incompatible usage. In consequence, most processing operations can take place without having to consider strict processing rules.

Directive 95/46	Safe Harbor
Article 7, CRITERIA FOR MAKING DATA PROCESSING LEGITIMATE Member States shall provide that personal data may be processed only if: (a) the data subject has unambiguously given his consent; or (b) processing is necessary for the performance of a contract to which the data subject is party or in order to take steps at the request of the data subject prior to entering into a contract; or (c) processing is necessary for compliance with a legal obligation to which the controller is subject; or (d) processing is necessary in order to protect the vital interests of the data subject; or (e) processing is necessary for the performance of a task carried out in the public interest or in the exercise of official authority vested in the controller or in a third party to whom the data are disclosed; or (f) processing is necessary for the purposes of the legitimate interests pursued by the controller or by the third party or parties to whom the data are disclosed, except where such interests are overridden by the interests for fundamental rights and freedoms of the data subject which require protection under Article 1 (1).	**NOTICE** An organization must inform individuals about the purposes for which it collects and uses information about them, how to contact the organization with any inquiries or complaints, the types of third parties to which it discloses the information, and the choices and means the organization offers individuals for limiting its use and disclosure. This notice must be provided in clear and conspicuous language when individuals are first asked to provide personal information to the organization or as soon thereafter as is practicable, but in any event before the organization uses such information for a purpose other than that for which it was originally collected or processed by the transferring organization or discloses it for the first time to a third party **CHOICE** An organization must offer individuals the opportunity to choose (opt out) whether their personal information is (a) to be disclosed to a third party or (b) to be used for a purpose that is incompatible with the purpose(s) for which it was originally collected or subsequently authorized by the individual. Individuals must be provided with clear and conspicuous, readily available, and affordable mechanisms to exercise choice.

b) Result of Comparison

The SHD follows a general processing approach which differs in essential points from EU data protection rules. In the EU processing of personal data is prohibited unless one of the explicitly listed exemptions applies.[20] Under SH, it is exactly the opposite. When applying the notice and choice principle, the general prohibition to process personal data is replaced by a general permission.

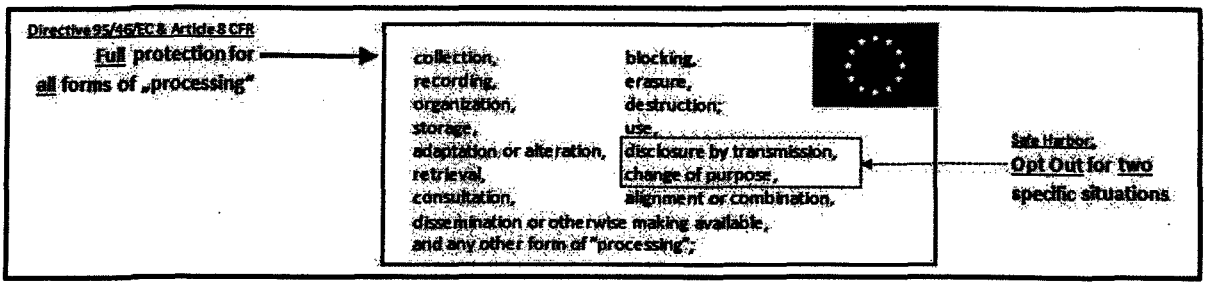
[20] Compare Boehm/Cole, Data Retention after the Judgement of the Court of Justice of the European Union, p. 49.

Analyzing the two principles in detail, doubts regarding the effectiveness of the protection occur. The information principle specifies the moment at which the US organization is obliged to inform the data subject. It says that the information must be provided when "individuals are first asked to provide personal information to the organization or as soon thereafter as is practicable". These options leave considerable space for misuse. The US organization does not ask individuals to provide personal information to them. Instead, it imports data that was provided to them by an organization in the EU.

This strange construction in the SHD at least leaves open the possibility that US organizations delay the application of the information principle and by doing so weaken the data subjects' rights.

Only if the receiving organization in the US "uses the information for a purpose other than that for which it was originally collected or processed by the transferring organization or discloses it for the first time to a third party", the SHD leaves no space for delaying the necessary information. In that case the organization in the US clearly has to notify the data subject before the mentioned actions are carried out. Nevertheless, this stricter obligation can also be circumvented if already the transferring organization formulates a very broad purpose[21] or if the notification requirement is overridden by US law. In consequence the information principle as one basic requirement for lawful data processing has considerable disadvantages compared to the standards guaranteed in the EU.

The structure of the second main principle, the choice principle, brings up further questions regarding the effectiveness of data protection in the US. It requires US organizations to offer data subjects the opportunity to "opt out" of specific processing operations. The option to opt out is an equivalent to the "right to object" in Article 14 of the Directive. It is applicable in only two situations, which are "usage for another purpose" or "disclosure to a third party". These situations can, however, be restricted by US law. Every other processing operation can be conducted by the organization. Consequently, the data subject has quite often no influence on the handling of its personal data.



Furthermore, the opt-out-method has next to its limited application another structural shortcoming. The opportunity to opt out must be "provided with clear and conspicuous, readily available, and affordable mechanisms to exercise choice". However, the determination that the data subject did not choose to opt out (when it comes to a change of purpose or disclosure to a third party) does not necessarily mean that it gave its consent to the processing operation. It is for example not unlikely that the data subject missed the option. This especially happens when a data subject faces a huge amount of information. Besides, it

[21] Compare for instance facebook, statement of rights and responsibilities, legal terms, para 17, available at: https://www.facebook.com/legal/terms.

is doubtful if the option to opt-out is similar to giving consent "unambiguously", which is required by Directive 95/46. While not opting-out means that a person behaves in a passive way, the approach in the Directive is based on activity by a person. From this observation one can conclude that SHD relies on a mechanism that at least cannot be regarded completely useful and effective for enforcing data protection standards. Against the background of this, the question arises why the application of the opt-out-method is limited to only a part of possible processing operations.

All things considered the protection of SH appears considerably lower than the minimal standards of Directive 95/46, Article 8 CFR ("data must be processed ... on the basis of the consent ... or some other legitimate basis laid down by law") and even the OECD guidelines (see "Use Limitation Principle").

3. Onward Transfer

a) General Remarks

Under Directive 95/46 the transfer of data respectively the "disclosure by transmission" constitutes a form of processing (Article 2 (b)). Therefore, the general limitations applicable to any "processing operation" apply. Transfers must be allowed under Articles 7 or 8 and the processing operation must fulfill the requirements of Article 6. Transfers outside of the area that is governed by Directive 95/46 (countries that are not members of the EU/EEA) fall under the additional limitations of Articles 25 and 26.

SH does not foresee any limitations on onward transfer other than "notice and choice", which effectively means that data subjects must have an option to "opt out" of an onward transfer. Moreover, these principles can be overridden by US law (see above). Only if the recipient acts as an "agent" ("processor"), an adequate level of protection has to be granted. In all other cases the recipient of the data is not required to provide any form of an "adequate protection".

Directive 95/46	Safe Harbor
Article 25, TRANSFER OF PERSONAL DATA TO THIRD COUNTRIES The Member States shall provide that the transfer to a third country of personal data which are undergoing processing or are intended for processing after transfer may take place only if, without prejudice to compliance with the national provisions adopted pursuant to the other provisions of this Directive, the third country in question ensures an adequate level of protection. [...] **Article 26** **Derogations** 1. By way of derogation from Article 25 and save where otherwise provided by domestic law governing particular cases, Member States shall provide that a transfer or a set of transfers of personal data to a third country which does not ensure an adequate level of protection within the meaning of	**ONWARD TRANSFER** To disclose information to a third party, organizations must apply the Notice and Choice Principles. *[The following section on "agents" refers to "processors" as defined in Article 2(e) of Directive 95/46/EC]* Where an organization wishes to transfer information to a third party that is acting as an agent, as described in the endnote, it may do so if it first either ascertains that the third party subscribes to the Principles or is subject to the Directive or another adequacy finding or enters into a written agreement with such third party requiring that the third party provide at least the same level of privacy protection as is required by the relevant Principles. If the organization complies with these requirements, it shall

Article 25 (2) may take place on condition that: (a) the data subject has given his consent unambiguously to the proposed transfer; or (b) the transfer is necessary for the performance of a contract between the data subject and the controller or the implementation of precontractual measures taken in response to the data subject's request; or (e) the transfer is necessary for the conclusion or performance of a contract concluded in the interest of the data subject between the controller and a third party; or (d) the transfer is necessary or legally required on important public interest grounds, or for the establishment, exercise or defence of legal claims; or (e) the transfer is necessary in order to protect the vital interests of the data subject; or (f) the transfer is made from a register which according to laws or regulations is intended to provide information to the public and which is open to consultation either by the public in general or by any person who can demonstrate legitimate interest, to the extent that the conditions laid down in law for consultation are fulfilled in the particular case. [...]	not be held responsible (unless the organization agrees otherwise) when a third party to which it transfers such information processes it in a way contrary to any restrictions or representations, unless the organization knew or should have known the third party would process it in such a contrary way and the organization has not taken reasonable steps to prevent or stop such processing.

b) Result of Comparison

Both regulations follow the approach that data generally may not leave a sphere of "adequate protection". Under SH this is realized by obliging US organizations to apply the notice and choice principles. Theoretically, the data subject should on the basis of these principles be in the position to prevent the onward transfer if it does not want it to happen. This could lead to the assumption that the protection standard is higher than in the EU, where a general allowance for transfers to countries with an adequate level of protection exists. In the SH framework it appears that the data subject can influence the handling of its data in every single case.

But practically, the shortcomings of the principles become clear in the situation of onward transfers. Especially the opt-out-method has a negative effect on data protection standards in these situations (see above). With regard to the right to opt out it is also unclear, whether it must be applied in a situation where a data subject has "agreed" to forwarding of data through signing terms, privacy policies or other kinds of consent forms far before it actually comes to the transfer. It is questionable if such forms constitute an "informed, specific and unambiguous consent".

Besides, it must be observed that there are many exceptions to the SH. For example, US laws may allow or require to forward data to entities that do not provide for any guarantee (see exceptions above). All in all there is a wide scope of situations where onward transfer may be allowed.

4. Summary Substantive Law Guarantees

At a first glance the SHD contains most of the important ideas and principles that are laid down in Directive 95/46 in order to grant sufficient material protection for data subjects. But a closer look reveals

several weaknesses that raise the question if the principles are principally adequate to European standards.

The comparison of the provisions regulating data quality led to the conclusion that the requirements are implemented just superficially in the SHD. Important elements that can be found in Directive 95/46 were not transposed into the SHD. The lack of those elements results in missing crucial minimum standards such as the possibility to conduct a proportionality test, the strict purpose limitation principle and the idea of data minimization.

The SHD also follows a general approach on the question of legitimacy of processing that is disadvantageous for individuals compared to the European standards. There is no general prohibition of data processing operations but only the obligation to apply the notice and choice principles. These two basic principles suffer from structural as well as practical problems.

The structural and practical problems within the principles also have an impact on the possibility to transfer data to third parties. Additionally, exceptions and vague terms in the SHD weaken an effective protection from the onward transfer of data.

Considering these observations, one can conclude that the material protection granted by the SHD does not even come close to the level of protection Directive 94/46 offers to data subjects.

III. RIGHTS OF DATA SUBJECTS

1. Right to Access/Erasure/Rectification/Blocking

a) General Remarks

The right of an individual to access personal data is laid down in Article 12 of Directive 95/46. The same article also refers to the right to erasure, rectification and blocking of data that does not comply with the requirements of Directive 95/46. These rights are further specified in the national laws of the member states, for instance, with regard to the duration and costs of access.

Under SH the rights to access, correction, amendment and deletion are mentioned in Annexes I and II (FAQ 8). Annex I refers to these rights while Annex II limits the access right established in Annex I to a great extent.

According to Annex II (FAQ 8), the right to access is "subject to the principle of proportionality or reasonableness" or may be limited to data that is "readily available and inexpensive to provide" if "the information requested is not sensitive or not used for decisions that will significantly affect the individual". Equally "confidential commercial information" is excluded, as well as cases where access is "likely to interfere with the safeguarding of important countervailing public interests". The companies may also charge costs of the access that are "not excessive" which (according to the FAQs) "may be useful in discouraging repetitive and vexatious requests". The time-limit to provide an answer is defined as "without excessive delay and within a reasonable time period".

In addition, the rights to deletion, correction and amendment are limited to data that is "inaccurate". In contrast to EU law, the rights do not refer to data that is processed illegally or in violation of the SH rules.[22] As long as the content of the information is correct, there is thus no possibility of obtaining a deletion, correction and amendment of the data. This clearly contradicts established EU data protection principles.[23] Moreover, there is no possibility to obtain access, erasure, rectification or blocking of data that is accessed by US surveillance programs or transferred to others due to other legal obligations mentioned above.[24]

Directive 95/46	Safe Harbor
Article 12, Right of access Member States shall guarantee every data subject the right to obtain from the controller: (a) without constraint at reasonable intervals and without excessive delay or expense: - confirmation as to whether or not data relating to him are being processed and information at least as to the purposes of the processing, the categories of data concerned, and the recipients or categories of recipients to whom the data are disclosed, - communication to him in an intelligible form of the data undergoing processing and of any available information as to their source, - knowledge of the logic involved in any automatic processing of data concerning him at least in the case of the automated decisions referred to in Article 15 (1); (b) as appropriate the rectification, erasure or blocking of data the processing of which does not comply with the provisions of this Directive, in particular because of the incomplete or inaccurate nature of the data; (c) notification to third parties to whom the data have been disclosed of any rectification, erasure or blocking carried out in compliance with (b), unless this proves impossible or involves a disproportionate effort.	**ACCESS** Individuals must have access to personal information about them that an organization holds and be able to correct, amend, or delete that information where it is inaccurate, except where the burden or expense of providing access would be disproportionate to the risks to the individual's privacy in the case in question, or where the rights of persons other than the individual would be violated. *See "FAQ 8 – Access" of Annex II of the Safe Harbor Decision for numerous vague limitations and exceptions.*

[22] Compare Annex I of the SHD.

[23] Compare, for instance, Article 12 of Directive 95/46; Compare Boehm/Cole, Data Retention after the Judgement of the Court of Justice of the European Union, p. 28 et seq.

[24] Compare Communication of the Commission on the functioning of SH, p. 16 et seq., in particular para 7.2; for earlier assessments compare: Impact Assessment Study prepared for the European Commission in 2008 by the Centre de Recherche Informatique et Droit ('CRID') of the University of Namur; Commission Staff Working Paper "The application of Commission Decision 520/2000/EC of 26 July 2000 pursuant to Directive 95/46 of the European Parliament and of the Council on the adequate protection of personal data provided by the Safe Harbour Privacy Principles and related FAQs issued by the US Department of Commerce", SEC (2002) 196, 13.12.2002 and Commission Staff Working Paper "The implementation of Commission Decision 520/2000/EC on the adequate protection of personal data provided by the Safe Harbour Privacy Principles and related FAQs issued by the US Department of Commerce", SEC (2004) 1323, 20.10.2004.

b) Result of Comparison

The rights of access, correction, amendment and deletion in SH are formulated similar to Article 12 of Directive 95/46, but they are lacking further determination as currently provided for in the national laws of the member states for the provisions of the Directive. Only the access right is specified in Annex II (FAQ 8). This specification provides for a wide variety of exceptions and limitations to the right of access. This is aggravated by the fact that the existing guidelines on the application of the access right in Annex II are rather vague and difficult to enforce.

It is also worth noting that the rights to have data deleted, corrected or amended are limited in SH and can only be exercised in relation to "inaccurate" data. This clearly limits the possibility of the individual to remedy data that may be illegally processed or processed against the rules of SH.

2. Information Duties

a) General Remarks

The regulation of information duties of SH and Directive 95/46 appear to be similar in essential points.

Directive 95/46	Safe Harbor
Article 10, INFORMATION TO BE GIVEN TO THE DATA SUBJECT **Information in cases of collection of data from the data subject** Member States shall provide that the controller or his representative must provide a data subject from whom data relating to himself are collected with at least the following information, except where he already has it: (a) the identity of the controller and of his representative, if any; (b) the purposes of the processing for which the data are intended; (c) any further information such as - the recipients or categories of recipients of the data, - whether replies to the questions are obligatory or voluntary, as well as the possible consequences of failure to reply, - the existence of the right of access to and the right to rectify the data concerning him in so far as such further information is necessary, having regard to the specific circumstances in which the data are collected, to guarantee fair processing in respect of the data subject. **Article 11** **Information where the data have not been obtained from the data subject** 1. Where the data have not been obtained from the data subject, Member States shall provide that the controller or his representative must at the time of undertaking the recording	**NOTICE** An organization must inform individuals about the purposes for which it collects and uses information about them, how to contact the organization with any inquiries or complaints, the types of third parties to which it discloses the information, and the choices and means the organization offers individuals for limiting its use and disclosure. This notice must be provided in clear and conspicuous language when individuals are first asked to provide personal information to the organization or as soon thereafter as is practicable, but in any event before the organization uses such information for a purpose other than that for which it was originally collected or processed by the transferring organization or discloses it for the first time to a third party (1). (1) It is not necessary to provide notice or choice when disclosure is made to a third party that is acting as an agent to perform task(s) on behalf of and under the instructions of the organization. The Onward Transfer Principle, on the other hand, does apply to such disclosures.

of personal data or if a disclosure to a third party is envisaged, no later than the time when the data are first disclosed provide the data subject with at least the following information, except where he already has it: (a) the identity of the controller and of his representative, if any; (b) the purposes of the processing; (c) any further information such as - the categories of data concerned, - the recipients or categories of recipients, - the existence of the right of access to and the right to rectify the data concerning him in so far as such further information is necessary, having regard to the specific circumstances in which the data are processed, to guarantee fair processing in respect of the data subject. 2. Paragraph 1 shall not apply where, in particular for processing for statistical purposes or for the purposes of historical or scientific research,[...]	

b) Result of Comparison

Directive 95/46 requires slightly more detailed information to guarantee a "fair processing" than the SH. However, the information that theoretically should be given to the data subject is similar in both instruments and can be regarded as providing an adequate level of protection. The Commission however, constituted in a recent report on the practical functioning of SH after the PRISM revelations that there are situations in which individuals "may not be made aware by [...] companies that their data may be subject to access" by third parties.[25] This leads to a practical enforcement problem, which can also influence the exercise of the access rights and therefore needs to be considered when comparing the two instruments. If individuals are not aware of the fact that their data is transferred to third parties, they may refrain from exercising their access right.

3. Summary Rights of the Data Subject

Comparing the rights of access, deletion, correction and amendment leads to the following conclusions: The right of access under SH in Annex I is formulated in a similar way as in Directive 95/46. This similarity however ends when looking at the wide exceptions provided for in Annex II of the SH. On the one hand, there are several possibilities to restrict the access right, on the other hand the conditions for access are not defined in a way to enable persons concerned to understand the necessary legal details to enforce the access right. In the EU, such details are included in the national laws of the member states.

In addition to the restricted access right, the rights of deletion, correction and amendment are limited to cases in which the data is "inaccurate". SH lacks a remedy in cases where data is simply illegally processed but not inaccurate. Dispute resolution bodies may require organizations to remove or delete data as a "sanction" but the data subject has no subjective right to the removal.

[25] Compare Communication of the Commission on the functioning of SH, p. 16 et seq., in particular para 7.3.

When comparing the right to information, there is no fundamental difference between the right of Directive 95/46 and the information that needs to be provided according to the SH rules. However, there seems to be rather a practical enforcement problem that partly leads to the situation that individuals "may not be made aware by those companies that their data may be subject to access" by third parties.[26] In consequence, individuals concerned may not be informed about all details regarding the processing of their data and may refrain from exercising their access rights simply because they are not aware of the extent to which their data is used.

IV. ENFORCEMENT

1. Remedies

a) General Remarks

One of the most important issues with regard to the effective enforcement of fundamental rights relates to the possibility to claim a remedy before independent courts in cases of violations of the respective rights. This right is entailed in the ECHR, in the CFR and concretized in Article 22 of Directive 95/46 that guarantees a right for judicial remedies before a court for violations of the right to data protection.[27] One essential requirement to comply with this right is that the remedies are effective meaning that the remedy must be "sufficiently certain not only in theory but also in practice and must be effective in practice as well as in law".[28] The remedies usually refer to proceedings to obtain injunctive relief and/or damages. The concrete application of this right is left to the respective legal system of each member state.

The SHD lists in in Annex IV examples for cases in which damages may be claimed in US law, but does not provide for any independent cause of action due to a violation of the right to data protection. As the right to data protection is not known in the US jurisdiction, an individual concerned would have to refer to the existing civil law claims in US law and to the more broad application of the right to privacy in US case law. Annex IV of the SHD particularly refers to cases of fraudulent misrepresentation of facts, opinions, intentions or law "for the purpose of inducing another to act or to refrain from action in reliance upon it"[29], but rarely lists cases in which damages are awarded for privacy violations. Moreover, as mentioned above, some of the laws that interfere with data protection rights of individuals do not

[26] Compare Communication of the Commission on the functioning of SH p. 16 et seq., in particular para 7.3.

[27] Article 13 ECHR in connection with another right and Article 47 CFR.

[28] Compare Guide to good practice in respect of domestic remedies, adopted by the Committee of Ministers of the Council of Europe on 18 September 2013, p. 12, which refers to the cases: McFarlane v. Ireland , App. No. 31333/06, 10 September 2010, paragraph 114; Riccardi Pizzati v. Italy , App. No. 62361/00, Grand Chamber judgment of 29 March 2006, paragraph 38; El-Masri v. "the former Yugoslav Republic of Macedonia" , App. No. 39630/09, 13 December 2012, paragraph 255; Kudła v. Poland, App. No. 30210/96, judgment of 26 October 2000, paragraph 152.

[29] Compare Annex IV A of the SHD.

allow for the protection of EU citizens. Therefore it seems to be difficult to enact a civil law claim in US law for EU citizens.

A more concrete dispute resolution procedure is established in Annex II of the SH. FAQ 11 refers to alternative dispute resolution bodies that should handle claims of EU citizens in the first place. These dispute resolution bodies can refer a case to the FTC. The bodies will examine whether a SH certified company violates section 5 of the Federal Trade Commission Act (FTC Act) which prohibits "unfair or deceptive acts or practices in or affecting commerce." Section 5 of the FTC Act applies "to all persons engaged in commerce, including banks". The main dispute resolution bodies in this field are TRUSTe and BBB (Better Business Bureaus).

Alternatively, companies can choose to collaborate with the EU Data Protection Panel which is competent to deal with SH claims in the framework of human resources data. This panel is composed of representatives of EU data protection authorities and very rarely used.[30]

Directive 95/46	Safe Harbor
Article 22 - Remedies Without prejudice to any administrative remedy for which provision may be made, inter alia before the supervisory authority referred to in Article 28, prior to referral to the judicial authority, Member States shall provide for the right of every person to a judicial remedy for any breach of the rights guaranteed him by the national law applicable to the processing in question. **Article 23 - Liability** 1. Member States shall provide that any person who has suffered damage as a result of an unlawful processing operation or of any act incompatible with the national provisions adopted pursuant to this Directive is entitled to receive compensation from the controller for the damage suffered. [...]	**ANNEX IV** **Damages for Breaches of Privacy, Legal Authorizations and Mergers and Takeovers in U.S. Law** Failure to comply with the safe harbor principles could give rise to a number of private claims depending on the relevant circumstances *(Examples, see Annex IV of the SHD for details)* **Annex II, FAQ No 11, Dispute Resolution and Enforcement** **FTC Action** The FTC has committed to reviewing on a priority basis referrals received from privacy self-regulatory organizations, such as BBBOnline and TRUSTe, and EU Member States alleging non-compliance with the Safe Harbor Principles to determine whether Section 5 of the FTC Act prohibiting unfair or deceptive acts or practices in commerce has been violated. *(Examples, see Annex II of the SHD for details)*

b) Result of Comparison

While Directive 95/46 establishes a basis for effective remedies in national laws, mainly in form of injunctive relieve and damages, SH refers to the existing US civil law claims and establishes an Alternative Dispute Resolution (ADR) mechanism with links to the FTC. The FTC, however, is restricted to examine possible violations of section 5 of the FTC Act. It does not have the legal authority to remedy cases beyond the scope of application of this section. It is therefore not possible to obtain a remedy in a case

[30] Compare Communication of the Commission on the functioning of SH, p. 13, in particular para 5.2.

which does not refer to unfair or deceptive acts or practices in commerce through the FTC. This concerns violations of the SH principles by, for instance, public authorities that may violate SH principles by massively accessing SH data.

In addition to this legal restraint, the ADR mechanism is not very effective in practice. Therefore the Commission, in its report on the functioning of SH, criticizes that the effectiveness of this mechanism is not proven.[31] The example of TRUSTe is given:

> "[...] that reported that it received 881 requests in 2010, but that only three of them were considered admissible, and grounded, and led to the company concerned being required to change its privacy policy and website. In 2011, the number of complaints was 879, and in one case the company was required to change its privacy policy".[32]

The restriction of investigation powers of the FTC to Section 5 of the FTC Act and the practical difficulties in enforcing violations through the ADR bodies lead to the assumption that remedies are not effective in practice in SH. This contradicts the EU understanding of an effective remedy that must be certain not only in theory but also in practice. In addition, these ADR bodies seem to "lack appropriate means to remedy cases of failure to comply with the [SH] principles".[33] In consequence, there are important shortcomings regarding not only the enforcement in practice, but also in theory concerning the means to remedy a possible violation of SH principles.

In addition to these figures, most of the ADR providers charge a considerable fee for consumers for filling a complaint. This contradicts the guarantees of SH which requires an affordable recourse mechanism.[34]

2. Notification/Prior Checking/Publicizing

a) General Remarks

Directive 95/46 requires mechanisms which guarantee control over data processing activities. Chapter IX of Directive 95/46 obliges data controllers to notify the supervisory authority or the data controller must appoint a data protection officer (currently only in Germany). Data processing presenting a specific risk to the rights of the individuals is subject to prior checking.

SH follows a completely different approach and does not include duties of general overview or checking. Instead the companies subscribing to SH apply a "self-certification" method, which means in practice that the oversight work carried out by the supervisory authority (or data protection official) in the EU is done by the organization itself in the US.

---

[31] Compare Communication of the Commission on the functioning of SH, p. 14, in particular para 6.1 and also Communication of the Commission on Rebuilding Trust in EU-US Data Flows, COM(2013) 846 final.

[32] Communication of the Commission on the functioning of SH, pp. 14-15, in particular para 6.1, footnote 46.

[33] Ibid, p. 10, in particular para 5.

[34] Ibid, p. 15, in particular para 6.1.

Directive 95/46	Safe Harbor
NOTIFICATION **Article 18 - Obligation to notify the supervisory authority** 1. Member States shall provide that the controller or his representative, if any, must notify the supervisory authority referred to in Article 28 before carrying out any wholly or partly automatic processing operation or set of such operations intended to serve a single purpose or several related purposes. [...] **Article 19 - Contents of notification** 1. Member States shall specify the information to be given in the notification. It shall include at least: [...] **Article 20 - Prior checking** 1. Member States shall determine the processing operations likely to present specific risks to the rights and freedoms of data subjects and shall check that these processing operations are examined prior to the start thereof. [...] **Article 21 - Publicizing of processing operations** 1. Member States shall take measures to ensure that processing operations are publicized. [...]	**FAQ 6 - Self-Certification** **Q: How does an organization self-certify that it adheres to the Safe Harbor Principles?** **A:** Safe harbor benefits are assured from the date on which an organization self-certifies to the Department of Commerce (or its designee) its adherence to the Principles in accordance with the guidance set forth below. To self-certify for the safe harbor, organizations can provide to the Department of Commerce (or its designee) a letter, signed by a corporate officer on behalf of the organization that is joining the safe harbor, that contains at least the following information: 1. name of organization, mailing address, e-mail address, telephone and fax numbers; 2. description of the activities of the organization with respect to personal information received from the EU; and 3. description of the organization's privacy policy for such personal information, including: (a) where the privacy policy is available for viewing by the public, (b) its effective date of implementation, (c) a contact office for the handling of complaints, access requests, and any other issues arising under the safe harbor, (d) the specific statutory body that has jurisdiction to hear any claims against the organization regarding possible unfair or deceptive practices and violations of laws or regulations governing privacy (and that is listed in the annex to the Principles), (e) name of any privacy programs in which the organization [...] **Q: How do organizations provide follow up procedures for verifying that the attestations and assertions they make about their safe harbor privacy practices are true and those privacy practices have been implemented as represented and in accordance with the Safe Harbor Principles?** **A:** To meet the verification requirements of the Enforcement Principle, an organization may verify such attestations and assertions either through self-assessment or outside compliance reviews. [...]

b) Result of Comparison

There is a fundamental difference when it comes to the control of data processing activities by data controller between the EU and the SH system. The self-certification mechanism of SH does not require any external control or review that ensures compliance with the SH principles. The self-certification is completed through a letter to the Department of Commerce with basic information about the organization. Follow up procedures can be equally carried out by the organization itself. There is also "no full evaluation of the actual practice in self-certified companies".[35] The Commission therefore requires "an active follow up by the Department of Commerce on effective incorporation of the Safe Harbour

[35] Compare Communication of the Commission on the functioning of SH, p. 8, in particular para 4.

principles [...]."[36] So far, a self-certified company comes only under scrutiny after an individual uses the enforcement mechanisms that are available to him.[37]

The lack of notification, prior checking and external control of the SH principles is hardly in compliance with the requirements of EU data protection rights. The Court of Justice regularly requires independent control of data processing activities to assure that basic rights are respected.[38] Refraining from one of the essential data protection requirements by accepting the SH self-certifying mechanism clearly interferes with the guarantees of Article 7 and 8 CFR and 8 ECHR and cannot be regarded as providing an adequate level of protection anymore.

3. Supervisory Authority/Enforcement

a) General Remarks

Connected to the notification and prior checking requirement is the exercise of independent control.[39] Article 28 of Directive 95/46 (together with the general principles of EU law, national laws and Article 8 III CFR) provides for the establishment of independent supervisory authorities in each member state. They are equipped with enforcement and investigations powers and must process complaints filed by data subjects. The supervisory authorities are described by the Court of Justice as "the guardians of [...] fundamental rights and freedoms, and their existence in the Member States is considered, as is stated in the 62nd recital in the preamble to Directive 95/46, as an essential component of the protection of individuals with regard to the processing of personal data."[40] They must be completely independent meaning that they must be free from any external influence. The mere risk that such influence could be exercised over the decisions of the supervisory authorities is "enough to hinder the latter authorities' independent performance of their tasks".[41]

As already seen above, SH only foresees the FTC as investigative authority, while "dispute resolution bodies" can only decide over complaints but lack power to investigate the facts. The ADR bodies are chosen and paid by the SH organization and therefore not independent in the sense of EU data protection law.

---

[36] Compare Communication of the Commission on the functioning of SH, p. 8, in particular para 4.

[37] According to the communication of the Commission on the functioning of SH, the FTC initiated 10 enforcement actions against self-certified SH companies until 2013, compare p. 10.

[38] Compare: C-518/07, Commission v. Germany of 9 March 2010 and case C-614/10, European Commission v. Republic of Austria of 16 Oct. 2012, Case C-288/12, European Commission v Hungary of 8 April 2014.

[39] Compare: C-518/07, Commission v. Germany of 9 March 2010 and case C-614/10, European Commission v. Republic of Austria of 16 Oct. 2012, Case C-288/12, European Commission v Hungary of 8 April 2014.

[40] C-518/07, Commission v. Germany of 9 March 2010, para 23.

[41] C-518/07, Commission v. Germany of 9 March 2010, para 36.

Data subjects may also direct their requests to the FTC, but the FTC is not obliged to investigate consumer complaints.[42] According to the Communication of the Commission on the functioning of SH, it seems that the FTC has so far only reviewed a few complaints of EU data protection authorities, but no complaints filed by EU data subjects.[43] The few enforcement actions taken by the FTC (10 until 2013) were also mainly based on interventions form EU bodies, or referred to broader violations of section 5 of the FTC Act in the privacy field.

Directive 95/46	Safe Harbor
Article 28, Supervisory authority 1. Each Member State shall provide that one or more public authorities are responsible for monitoring the application within its territory of the provisions adopted by the Member States pursuant to this Directive. [...] 3. Each authority shall in particular be endowed with: - investigative powers, such as powers of access to data forming the subject-matter of processing operations and powers to collect all the information necessary for the performance of its supervisory duties, - effective powers of intervention, such as, for example, that of delivering opinions before processing operations are carried out, in accordance with Article 20, and ensuring appropriate publication of such opinions, of ordering the blocking, erasure or destruction of data, of imposing a temporary or definitive ban on processing, of warning or admonishing the controller, or that of referring the matter to national parliaments or other political institutions, - the power to engage in legal proceedings where the national provisions adopted pursuant to this Directive have been violated or to bring these violations to the attention of the judicial authorities. Decisions by the supervisory authority which give rise to complaints may be appealed against through the courts. [...]	**ENFORCEMENT** Effective privacy protection must include mechanisms for assuring compliance with the Principles, recourse for individuals to whom the data relate affected by non-compliance with the Principles, and consequences for the organization when the Principles are not followed. At a minimum, such mechanisms must include (a) readily available and affordable independent recourse mechanisms by which each individual's complaints and disputes are investigated and resolved by reference to the Principles and damages awarded where the applicable law or private sector initiatives so provide; (b) follow up procedures for verifying that the attestations and assertions businesses make about their privacy practices are true and that privacy practices have been implemented as presented; and (c) obligations to remedy problems arising out of failure to comply with the Principles by organizations announcing their adherence to them and consequences for such organizations. [...]

b) Result of Comparison

While Directive 95/46 as well as Article 8(3) CFR require a completely independent supervisory authority equipped with investigation and enforcement powers, the SH provides for the dispute resolution mechanism which shifts the control of the SH principles to private organizations that are chosen and paid by the SH companies. These organizations do not have investigative powers and cannot be regarded as independent within the meaning of EU law. Moreover, they do not exercise an active control over data processing activities of the SH companies; they only react to complaints of consumers. This concept is

[42] Compare: A Brief Overview of the Federal Trade Commission's Investigative and Law Enforcement Authority: http://www.ftc.gov/about-ftc/what-we-do/enforcement-authority and https://www.ftccomplaintassistant.gov/#crnt&panel1-1 that says: "The FTC cannot resolve individual complaints, but we can provide information about what next steps to take".

[43] Communication of the Commission on the functioning of SH, p. 11, para 5.1.

totally different from the EU understanding of independent control, which is in various cases a proactive control to prevent fundamental rights' violations before they arise.

There is also the possibility to refer a complaint to the FTC, which has however so far not investigated a complaint of an EU consumer.

4. Sanctions

a) General Remarks

Directive 95/46 requires Member States to lay down sanctions for breaches of the directive. The sanctions are set by each Member State and vary greatly (e.g. up to € 25.000 - or even imprisonment in certain cases - in Austria; up to € 100.000 in Ireland; up to € 300.000 or even higher in Germany).

The SHD establishes a stepwise sanction system. As a first step it is laying the task to sanction violations on "dispute resolution bodies". These can choose from sanctions that vary in their degree of severity. The SHD lists sanctions like "public findings of non-compliance", "requirements to delete data", "suspension or removal of a seal", "compensation for losses" or "injunctive orders". Failures to comply with these rulings must be notified not only to the Department of Commerce but also to the governmental body with applicable jurisdiction or to courts.

As a second step, violations can be indirectly sanctioned by the FTC through its authority in Section 5 of the FTC act. If the FTC concludes that Section 5 has been violated, it may "resolve the matter by seeking an administrative cease and desist order prohibiting the challenged practices or by filing a complaint in a federal district court, which if successful could result in a federal court order to the same effect" (FAQ 11). If the administrative or the federal orders are violated, the FTC may obtain civil penalties or pursue civil or criminal contempt.

A further step would be an action due to "persistent failure to comply with the principles". FAQ 11 explains this behavior more detailed. "Persistent failure to comply" may be actionable under the False Statements Act (18 U.S.C. § 1001) with up to five years of imprisonment.

Directive 95/46/EC	Safe Harbor
Article 24, SANCTIONS The Member States shall adopt suitable measures to ensure the full implementation of the provisions of this Directive and shall in particular lay down the sanctions to be imposed in case of infringement of the provisions adopted pursuant to this Directive.	**ENFORCEMENT** [...] Sanctions must be sufficiently rigorous to ensure compliance by organizations. **FAQ 11: Remedies and Sanctions.** The result of any remedies provided by the dispute resolution body should be that the effects of non-compliance are reversed or corrected by the organization, in so far as feasible, and that future processing by the organization will be in conformity with the Principles and, where appropriate, that processing of the personal data of the individual who has brought the complaint will cease.

	Sanctions need to be rigorous enough to ensure compliance by the organization with the Principles. [...] Sanctions should include both publicity for findings of non-compliance and the requirement to delete data in certain circumstances. Other sanctions could include suspension and removal of a seal, compensation for individuals for losses incurred as a result of non-compliance and injunctive orders. [...]

b) Result of Comparison

Both systems require sanctions. However, the "sanctions" provided for in the SHD at first step are mainly remedies. According to the 2013 annual report of the largest dispute resolution body (TRUSTe), companies are usually only required to change their policy, sanctions are not imposed.[44]

Under the FTC act and the False Statements Act more severe actions can be initiated. The provisions are supposedly in conformity with the provisions in the Directive. Nevertheless, the system that is implemented is quite different. It is not only complicated but relies also in large parts on the participation of dispute resolution bodies and the concerned organizations.

In consequence, it seems doubtful that the FTC (or the Department of Commerce) initiates proceedings of its own accord. In practice, all but one of the enforcement actions so far led to "settlements" between the FTC and organizations that violated the SH; a fine on the respective organization was not imposed.[45]

5. Summary Enforcement

Comparing the enforcement mechanisms of Directive 95/46 and the SH rules, doubts arise regarding the effective enforcement of remedies, sanctions and notification duties as well as the establishment of independent supervisory bodies within the SH framework.

With regard to effective remedies, it is doubtful whether the limited jurisdiction of the FTC and the ADR mechanism, which faces practical enforcement difficulties, can be classified as adequate according to the criteria mentioned in Article 25 (2) of Directive 95/46. The SH does not expressly establish a new cause of action for damages or an injunctive relief, contrary to the requirements of Directive 95/46. Instead Annex IV of the SHD only refers to the general US civil law and does not indicate that SH itself is enforceable. In addition to such legal uncertainties, individuals may also face practical difficulties when it comes to travel, costs and language barriers in case of civil law claims. The theoretical as well as the practical enforcement of remedies in the SH framework is thus very limited.

A comparison of the control mechanisms reveals further fundamental differences. While the control of data processing activities in the EU includes notification, prior checking and external control of such activities, the SH establishes a self-certifying mechanism which largely refrains from external control procedures. Dispute resolution bodies, for instance, are chosen by the organizations processing the data

[44] TRUSTe Transparency Report 2013, available at: http://www.truste.com/window.php?url=http://download.truste.com/TVarsTf=3L0AXBJ0-470.

[45] Compare figure 1.

and can therefore not be regarded as independent within the meaning of EU law.[46] According to EU law, only independent control mechanisms can assure compliance with data protection and privacy rights. Thus, the concept of control over data processing activities in SH is contrary to the concept established by Directive 95/46 and Article 8 CFR.

In contrast to the ADR bodies, the FTC is an independent organization, which is equipped with investigative powers. Its investigations can lead to sanctions being imposed on the companies violating section 5 of the FTA Act. Sanctions are, however, very rare.[47] Moreover, the FTC is usually not actively reviewing and investigating the factual practices of companies. Further, complaints by individual data subjects are not investigated in practice. In summary, there are serious doubts on the SH adequacy finding with regard to enforcement. Criticism refers mainly to the non-effective enforcement of remedies and the self-controlling mechanism when it comes to oversight and control mechanisms over data processing activities within the SH framework. Therefore, the existing procedures do not to satisfy the EU requirements with regard to enforcement.

Figure 1: registration settlements in context with SH (2014)

Registration Settlements (2014)			
1 ExpatEdge Partners, LLC, FTC File No. 0923138	November 9, 2009	Certification Lapsed	settled: prohibition from further misrepresentations, no fine
2 Onyx Graphics, Inc., FTC File No. 0923139	November 9, 2009	Certification Lapsed	settled: prohibition from further misrepresentations, no fine
3 Progressive Gaitways LLC, FTC File No. 0923141	November 9, 2009	Certification Lapsed	settled: prohibition from further misrepresentations, no fine
4 Collectify LLC, FTC File No. 0923142	November 9, 2009	Certification Lapsed	settled: prohibition from further misrepresentations, no fine
5 World Innovators, Inc., FTC File No. 0923137	January 12, 2010	Certification Lapsed	settled: prohibition from further misrepresentations, no fine
6 Directors Desk LLC, FTC File No. 0923140	January 12, 2010	Certification Lapsed	settled: prohibition from further misrepresentations, no fine
7 Javian Karnani, and Balls of Kryptonite, LLC, Civ. No. 095276	May 16, 2011	Mainly: Online Fraud, SH: Not	settled: prohibition from further misrepresentations, $ 500.000
Material Settlements (2011-12)			
8 Google Inc., FTC File No. 1023136	March 30, 2011	Sec. 5 FTC Act & SH	settled: no further misrepresentation, improvements, external
9 Facebook, Inc., FTC File No. 0923184	November 29,	Sec. 5 FTC Act & SH	settled: no further misrepresentation, improvements, external
10 My Space, LLC, FTC File No. 1023058	May 8, 2012	Sec. 5 FTC Act & SH	settled: no further misrepresentation, external audits, no fine
Registration Settlements (2014)			
11 American Apparel, Inc., FTC File No. 1423036	June 25, 2014	Certification Lapsed	settled: prohibition from further misrepresentations, no fine
12 Apperian, Inc., FTC File No. 1423017	June 25, 2014	Certification Lapsed	settled: prohibition from further misrepresentations, no fine
13 Atlanta Falcons Football, LLC., FTC File No. 1423018	June 25, 2014	Certification Lapsed	settled: prohibition from further misrepresentations, no fine
14 Baker Tilly Virchow Krause, LLP, FTC File No. 1423019	June 25, 2014	Certification Lapsed	settled: prohibition from further misrepresentations, no fine
15 BitTorrent, Inc., FTC File No. 1423020	June 25, 2014	Certification Lapsed	settled: prohibition from further misrepresentations, no fine
16 Charles River Labs International, Inc., FTC File No. 1423022	June 25, 2014	Certification Lapsed	settled: prohibition from further misrepresentations, no fine
17 DataMotion, Inc., FTC File No. 1423023	June 25, 2014	Certification Lapsed	settled: prohibition from further misrepresentations, no fine
18 DDC Laboratories, Inc., FTC File No. 1423024	June 25, 2014	Certification Lapsed	settled: prohibition from further misrepresentations, no fine
19 Fantage, Inc., FTC File No. 1423026	June 25, 2014	Certification Lapsed	settled: prohibition from further misrepresentations, no fine
20 Level 3 Communications, LLC, FTC File No. 1423028	June 25, 2014	Certification Lapsed	settled: prohibition from further misrepresentations, no fine
21 PBD Sports, Ltd. d/b/a Denver Broncos Football Club, FTC File No.	June 25, 2014	Certification Lapsed	settled: prohibition from further misrepresentations, no fine
22 Reynolds Consumer Products, Inc., FTC File No. 1423030	June 25, 2014	Certification Lapsed	settled: prohibition from further misrepresentations, no fine
23 Receivables Management Services Corporation, FTC File No. 1423031	June 25, 2014	Certification Lapsed	settled: prohibition from further misrepresentations, no fine
24 Tennessee Football, Inc., FTC File No. 1423032	June 25, 2014	Certification Lapsed	settled: prohibition from further misrepresentations, no fine

[46] Compare cases C-518/07, Commission v. Germany of 9 March 2010 and case C-614/10, European Commission v. Republic of Austria of 16 Oct. 2012, Case C-288/12, European Commission v Hungary of 8 April 2014 in which the Court of Justice clarified that the mere risk of influence being exercised over supervisory authorities is enough to violate the independency requirement.

[47] Compare figure 1; there is one case in 2012 in which google paid 22, 5 Million Dollar to settle FTC charges, however, these charges were not related to a safe harbor violation, compare: http://www.ftc.gov/news-events/press-releases/2012/08/google-will-pay-225-million-settle-ftc-charges-it-misrepresented.

V. FINAL REMARKS

The comparison between the guarantees of SH and Directive 95/46 shows considerable differences concerning the protected rights of individuals. In particular, the self-certifying mechanism and the applicability of US law when it comes to questions of interpretation of SH lead to a lack of protection for EU citizens if their data is transferred under SH. As every rule of the federal, state or even the local level existing in the US can override the guarantees of the SHD, there is no comprehensive protection for the rights of individuals in SH.

Comparing the enforcement mechanisms of Directive 95/46 and the SH rules, doubts arise regarding the effective enforcement of remedies, sanctions and notification duties as well as the establishment of independent supervisory bodies within the SH framework. It is very doubtful whether the limited jurisdiction of the FTC and the ADR mechanism, which faces various difficulties, can be classified as adequate according to the criteria mentioned in Article 25 (2) of Directive 95/46. The lack of independent and active control over data processing activities is also in contrast to established EU law.

The rules on onward transfer allow for a wide ranging use of data outside the "sphere of protection" of SH. Restrictions and limitations of the fundamental rights of EU citizens go far beyond of what is tolerated in the EU. Such limitations do not even require a proportionality or balancing test between the different interests at stake. This constitutes a clear violation of Article 7, 8 and 52 (1) CFR and the ECHR and can therefore not be regarded as adequate.

Crucial elements with regard to data quality such as fairness, lawfulness, adequacy, explicit purpose limitation that result from Directive 95/46, Article 7, 8 CFR and Article 8 ECHR are not applied at all or applied in a less strict way. Legitimate processing depends on the notice and choice principles which are limited in its application and can also be overridden by US law.

In addition, the rights to deletion, correction and amendment are limited to data that is "inaccurate". In contrast to EU law, the rights do not refer to data that is processed illegally or in violation of the SH rules. This clearly limits the possibility of the individual to remedy data that may be illegally processed or processed against the rules of SH. Moreover, there is no possibility to obtain access, erasure, rectification or blocking of data that is accessed by US surveillance programs or transferred to others due to other legal obligations mentioned in the opinion.

In summary, there are serious doubts on the adequacy finding of the SH as it could be observed that the SHD is differing in essential points from minimum European data protection standards that are laid down in Directive 95/46.

[redacted]

Signature

Franziska Boehm

The opinion was requested by the applicant. Funding was not provided.

WE HEREBY CERTIFY THE WITHIN TO BE TRUE COPY OF THE ORIGINAL

[redacted]

GERARD RUDDEN
SOLICITOR
5 CLARE ST.
DUBLIN 2

CASE C-362/14

MAXIMILLIAN SCHREMS

Applicant

V.

DATA PROTECTION COMMISSIONER

Respondent

AND

DIGITAL RIGHTS IRELAND LIMITED

Amicus curiae

Annex A.2

Complaint by Max Schrems to TRUSTe and response of TRUSTe.

Von: TRUSTe Feedback and Resolution System <consumer-feedback@feedback.truste.com>
Gesendet: Donnerstag, 28. November 2013 21:13
An: Max Schrems
Betreff: Request received: #28321: www.facebook.com

TRUSTe

Ticket #28321: www.facebook.com

Dear Maximilian Schrems,

Thank you for submitting your report via TRUSTe's Feedback and Resolution System. Your request (#28321) has been received, and is being reviewed. We will contact you within the next 14 calendar days concerning the next steps (usually it only takes 1-2 business days, but can take longer depending on the volume of reports TRUSTe is handling).

If you have any additional questions or comments concerning your complaint, please reply to this email directly, or follow the link below:
http://feedback.truste.com/requests/28321

Sincerely,
TRUSTe Compliance Team

Max Schrems, Nov 28 12:13 (PST):

See Attachment or download here:
http://www.europe-v-facebook.org/ljdklsdhksdhklhadhljdh1782sjel2937ljels.pdf

This email is a service from TRUSTe Feedback and Resolution System.

Von: TRUSTe Feedback and Resolution System <consumer-feedback@feedback.truste.com>
Gesendet: Montag, 02. Dezember 2013 21:54
An: Max Schrems
Betreff: Re: TRUSTe #28321: www.facebook.com

TRUSTe

Ticket #28321: www.facebook.com

Dear Maximilian Schrems,

TRUSTe Compliance 2, Dec 02 12:54 (PST):

Thank you for contacting TRUSTe. TRUSTe does not own or operate Facebook, though we do provide privacy-related dispute resolution services for Facebook.

As you may be aware, Facebook's privacy policy includes a notice to consumers that it may share consumer data as follows:

"We may access, preserve and share your information in response to a legal request (like a search warrant, court order or subpoena) if we have a good faith belief that the law requires us to do so. This may include responding to legal requests from jurisdictions outside of the United States where we have a good faith belief that the response is required by law in that jurisdiction, affects users in that jurisdiction, and is consistent with internationally recognized standards. We may also access, preserve and share information when we have a good faith belief it is necessary to: detect, prevent and address fraud and other illegal activity; to protect ourselves, you and others, including as part of investigations; or to prevent death or imminent bodily harm."

You requested the following resolution:
"Stop Facebook Inc's involvement in PRISM."

TRUSTe does not have authority to address the matter you raise. We are therefore closing this issue in our system as being outside the scope of TRUSTe's authority.

--TRUSTe Compliance Team

Sincerely,

TRUSTe Compliance Team

Von: TRUSTe Feedback and Resolution System <consumer-feedback@feedback.truste.com>
Gesendet: Montag, 02. Dezember 2013 22:10
An: Max Schrems
Betreff: Re: TRUSTe #28321: www.facebook.com

TRUSTe

Ticket #28321: www.facebook.com

Dear Maximilian Schrems:

Thank you for your recent reply through TRUSTe's Feedback and Resolution System.

Once a ticket has been closed in our system, sending correspondence to this address will not reopen it.

If you feel that this matter should be reopened because there is still an unresolved issue within the scope of TRUSTe's program and you would like to appeal our decision, please email appeals@truste.com with your ticket number and a description as to why this issue should not be closed (for example, if you believe TRUSTe misunderstood an aspect of what you are reporting, erred in interpreting our program requirements, or if you received new information that was not previously available).

To learn more about the appeals process, please visit:
http://www.truste.com/why_TRUSTe_privacy_services/online-privacy-watchdog.html

Thank you for contacting TRUSTe.

This email is a service from TRUSTe Feedback and Resolution System.

Von: TRUSTe Feedback and Resolution System <consumer-feedback@feedback.truste.com>
Gesendet: Montag, 02. Dezember 2013 22:20
An: Max Schrems
Betreff: Re: TRUSTe #28321: www.facebook.com

TRUSTe

Ticket #28321: www.facebook.com

Dear Maximilian Schrems,

TRUSTe Compliance 2, Dec 02 13:19 (PST):

TRUSTe has received the message below to appeals@truste.com. In accordance with our process, this ticket has been reopened pending further review by TRUSTe of the message below.

--TRUSTe Compliance Team

---------- Forwarded message ----------
From:
Date: Mon, Dec 2, 2013 at 1:14 PM
Subject: AW: TRUSTe #28321: www.facebook.com
To: appeals@truste.com

To whom it may concern.

Thank you for your response – as I expected it to be.
Who has the authority to take action, if not TRUSTe?

You are not saying why you do not have any authority under "Safe Harbour".
I do not really care about the policy of Facebook, as I claimed that is violates "Safe Harbour", not its policy.

Can you comment on this?

Kind Regards,

Maximilian Schrems

Sincerely,

TRUSTe Compliance Team

Von: TRUSTe Feedback and Resolution System <consumer-feedback@feedback.truste.com>
Gesendet: Mittwoch, 04. Dezember 2013 04:10
An: Max Schrems
Betreff: Re: TRUSTe #28321: www.facebook.com

TRUSTe

Ticket #28321: www.facebook.com

Dear Maximilian Schrems,

TRUSTe Compliance 2, Dec 03 19:10 (PST):

Thank you for contacting appeals@truste.com. This matter is not something governed by our privacy program. We are therefore closing this issue in TRUSTe's system.

--TRUSTe Compliance Team

Sincerely,

TRUSTe Compliance Team

This email is a service from TRUSTe Feedback and Resolution System.

WE HEREBY CERTIFY THE WITHIN TO BE TRUE COPY OF THE ORIGINAL

[redacted]
GERARD RUDDEN
SOLICITOR
5 CLARE ST.
DUBLIN 2

CASE C-362/14

MAXIMILLIAN SCHREMS

Applicant

V.

DATA PROTECTION COMMISSIONER

Respondent

AND

DIGITAL RIGHTS IRELAND LIMITED

Amicus curiae

Annex A.3

Complaint by Max Schrems to the US Federal Trade Commission (to date unanswered).

FEDERAL TRADE C MISSION

We have received your complaint.

Thank you for filing a complaint with the Federal Trade Commission. Based on the information you have given us, we recommend that you take the following steps, if you have not already.

Step: 1
You may find useful information on our Consumer Protection website .

Step: 2
If you have done the above steps and have any additional questions or any additional information you would like to add to your file, please call **877-382-4357** to speak with a counselor. When you call, please have this reference number: 50954602 to help us quickly retrieve your information.

You Might Also Like

Here are some additional links that will provide some useful information.

Online Shopping Tips (Video)
Computer Security (Video)
Solving Consumer Problems
Comparing Products Online
Computer Security

Print
Related Items

- About Us
- Getting Your Money Back
- Scam Alerts
- 10 Ways to Avoid Fraud

WE HEREBY CERTIFY THE WITHIN TO BE TRUE COPY OF THE ORIGINAL

[redacted]
GERARD RUDDEN
SOLICITOR
5 CLARE ST.
DUBLIN 2

CASE C-362/14

MAXIMILLIAN SCHREMS

Applicant

V.

DATA PROTECTION COMMISSIONER

Respondent

AND

DIGITAL RIGHTS IRELAND LIMITED

Amicus curiae

Annex A.4

List of FTC Decisions in the context of Safe Harbor Matters to date (format Excel)

[redacted]				
1	Expertdoc Partners, LLC, FTC File No. 0923138	November 9, 2009	Certification Lapsed	settled: prohibition from further misrepresentations, no fine
2	Onyx Graphics, Inc., FTC File No. 0923139	November 9, 2009	Certification Lapsed	settled: prohibition from further misrepresentations, no fine
3	Progressive Gateways LLC, FTC File No. 0923141	November 9, 2009	Certification Lapsed	settled: prohibition from further misrepresentations, no fine
4	[redacted] LLC, FTC File No. 0923142	November 9, 2009	Certification Lapsed	settled: prohibition from further misrepresentations, no fine
5	World Innovators, Inc., FTC File No. 0923137	January 12, 2010	Certification Lapsed	settled: prohibition from further misrepresentations, no fine
6	[redacted] Desk LLC, FTC File No. 0923140	January 12, 2010	Certification Lapsed	settled: prohibition from further misrepresentations, no fine
7	[redacted] and Sale of [redacted], LLC, Civ. No. 095276	May 16, 2011	Mainly: Online Fraud, SH: Not Certified	settled: prohibition from further misrepresentations, $ 500.000 (suspended)
[redacted]				
8	Google Inc., FTC File No. 1023136	March 30, 2011	Sec. 5 FTC Act & SH	settled: no further misrepresentation, improvements, external autdits, no fine
9	Facebook, Inc., FTC File No. 0923184	November 29, 2011	Sec. 5 FTC Act & SH	settled: no further misrepresentation, improvements, external autdits, no fine
10	My Space, LLC, FTC File No. 1023058	May 8, 2012	Sec. 5 FTC Act & SH	settled: no further misrepresentation, external autdits, no fine
[redacted]				
11	American Apparel, Inc., FTC File No. 1423036	June 25, 2014	Certification Lapsed	settled: prohibition from further misrepresentations, no fine
12	Apperian, Inc., FTC File No. 1423017	June 25, 2014	Certification Lapsed	settled: prohibition from further misrepresentations, no fine
13	Atlanta Falcons Football, LLC., FTC File No. 1423018	June 25, 2014	Certification Lapsed	settled: prohibition from further misrepresentations, no fine
14	Baker Tilly Virchow Krause, LLP, FTC File No. 1423019	June 25, 2014	Certification Lapsed	settled: prohibition from further misrepresentations, no fine
15	BitTorrent, Inc., FTC File No. 1423020	June 25, 2014	Certification Lapsed	settled: prohibition from further misrepresentations, no fine
16	Charles River Labs International, Inc., FTC File No. 1423022	June 25, 2014	Certification Lapsed	settled: prohibition from further misrepresentations, no fine
17	DataMotion, Inc., FTC File No. 1423023	June 25, 2014	Certification Lapsed	settled: prohibition from further misrepresentations, no fine
18	DDC Laboratories, Inc., FTC File No. 1423024	June 25, 2014	Certification Lapsed	settled: prohibition from further misrepresentations, no fine
19	Fantage, Inc., FTC File No. 1423026	June 25, 2014	Certification Lapsed	settled: prohibition from further misrepresentations, no fine
20	Level 3 Communications, LLC, FTC File No. 1423028	June 25, 2014	Certification Lapsed	settled: prohibition from further misrepresentations, no fine
21	PBD Sports, Ltd. d/b/a Denver Broncos Football Club, FTC File No. 1423025	June 25, 2014	Certification Lapsed	settled: prohibition from further misrepresentations, no fine
22	Reynolds Consumer Products, Inc., FTC File No. 1423030	June 25, 2014	Certification Lapsed	settled: prohibition from further misrepresentations, no fine
23	Receivables Management Services Corporation, FTC File No. 1423031	June 25, 2014	Certification Lapsed	settled: prohibition from further misrepresentations, no fine
24	Tennessee Football, Inc., FTC File No. 1423032	June 25, 2014	Certification Lapsed	settled: prohibition from further misrepresentations, no fine